On Ternary Monomial Substitution-Groups of Finite Order with Determinant ± 1.

BY ERNEST BROWN SKINNER.

INTRODUCTION.

The finite ternary linear substitution-groups generated by the two elements

$$S: \quad z'_i = z_{i+1}, \qquad T: \quad z'_i = a_i z_i,$$

$i = 1, 2, 3$, $a_1 a_2 a_3 = 1$ and $i + 1$ is taken mod 3, have been studied by Professor H. Maschke under the title "On Ternary Substitution-Groups of Finite Order which leave a Triangle Unchanged."*

Substitutions of the form

$$z'_i = a_i z_j \qquad (i, j = 1, 2, 3)$$

he has called *monomial substitutions* and the groups containing only such substitutions *monomial groups*. In what follows it is proposed to investigate all ternary monomial groups of finite order with determinant ± 1.

It is shown first, that the groups composed of multiplicative substitutions with determinant $+1$ may be generated by at most two substitutions, and conversely. The form of these independent generators is given explicitly. It is further shown that the ternary monomial groups with determinant ± 1 may be generated by at most three independent generators, one of which is of order 2, and conversely. It follows directly that the various types of groups to be studied are known. If T_1, T_2 and τ denote the generators of the ternary multiplicative group with determinant ± 1, and $S = (1, 2, 3)$, $s = (12)$, these types are found by taking every possible combination of the substitutions T_1, T_2, S, s, τ as generating operations.

In the second place, the sets of invariant forms of these groups have been

* American Journal of Mathematics, vol. XVII, No. 2.

determined in all cases, and the full systems have been worked out in all except certain exceptional cases (see §§6 and 12 below), for which only what Professor Maschke has has called "reduced systems," have as yet been found. In these exceptional cases, while the full systems have not been found in general terms, it is shown how in any case given numerically, the forms of the full system may readily be picked out.

Finally, the orders of the various groups are given in terms of the auxiliary quantities which occur in the solution of the problems to determine the invariant systems.

CHAPTER I.

TERNARY MONOMIAL GROUPS WITH DETERMINANT $+1$.

§1.—*Definitions and Notation.*

A multiplicative ternary substitution is a monomial substitution of the form

$$z_i' = a_i z_i,$$

a_i a root of unity and $a_1 a_2 a_3 = 1$.

Such substitutions may be denoted conveniently by

$$T = (\omega_{m_1}^{k'_1}, \quad \omega_{m_2}^{k'_2}, \quad \omega_3^{k'_3}),$$

or more briefly by

$$T = (\omega_m^{k_i}), \qquad i = 1, 2, 3, \qquad (2)$$

where $m =$ L. C. M. of m_1, m_2, m_3, and ω_m is a primitive with root of unity.

The subscript m is then the order of T and the determinant is $\omega_m^{\Sigma k} = \pm 1$.

If the determinant is $+1$

$$\Sigma k_i \equiv 0, \text{ (mod } m). \qquad (3)$$

If it is ± 1

$$\Sigma 2k_i \equiv 0, \text{ (mod } m). \qquad (4)$$

No two of the exponents k_i have a common divisor, which is, at the same time, a divisor of m. Two or more multiplicative substitutions T_1, T_2 .... are said to be independent if there exists no relation of the form

$$T_1^{\alpha} T_2^{\beta} \ldots . = 1,$$

α, β .... not multiples of the respective orders of T_1, T_2 ....

The necessary and sufficient conditions for the equality of two multiplica-

tive substitutions $T^{\alpha} = (\omega_m^{k_i})^{\alpha}$ and $T'^{\beta} = (\omega_m^{k_i'})^{\beta}$ of order m and both of determinant $+1$, are

$$\left.\begin{array}{l} k_i\alpha - k_i'\beta \equiv 0, \\ k_j\alpha - k_j'\beta \equiv 0, \end{array}\right\} \pmod{m} \qquad i, j = 1, 2, 3 \quad i \neq j. \quad (5)$$

§2.—*Groups of Ternary Multiplicative Substitutions with Determinant* $+1$.

Groups of multiplicative substitutions are evidently Abelian.

THEOREM I.—*The necessary and sufficient condition that two ternary multiplicative substitutions* $T_1 = (\omega_{N_1}^{k_i})$ *and* $T_2 = (\omega_{N_2}^{k'_i})$ *are independent, is that the two-rowed determinants of the matrix*

$$\left\| \begin{array}{ccc} k_1, & k_2, & k_3 \\ k_1', & k_2', & k_3' \end{array} \right\|$$

are prime to $d = [N_1, N_2]$.

If one of these determinants is prime to d, the other two are also by reason of the two relations

$$\Sigma k_i \equiv \Sigma k_i \equiv 0, \pmod{d}.$$

Suppose first that $N_1 = N_2 = d$. The conditions for

$$T_1^{\alpha} T_2^{\beta} = 1$$

are

$$\left.\begin{array}{l} k_1\alpha + k_1'\beta \equiv 0, \\ k_2\alpha + k_2'\beta \equiv 0, \end{array}\right\} \pmod{d}. \quad (6)$$

If $(k_1 k_2') = \Delta$, then

$$\left.\begin{array}{l} \Delta\alpha \equiv 0, \\ \Delta\beta \equiv 0, \end{array}\right\} \pmod{d}.$$

If $[\Delta, d] \neq 1$, there exists a solution of (6) such that α and β are both less than d. If $[\Delta, d] = 1$, there exists no solution of (6) except $\alpha \equiv \beta \equiv 0 \pmod{d}$. The condition is therefore necessary and sufficient when $N_1 = N_2$.

If $N_1 \neq N_2$, let $N_1 = r_1 d$, $N_2 = r_2 d$, $T_1^{r_1} = (\omega_d^{\bar{k}_i})$ and $T_2^{r_2} = (\omega_d^{\bar{k}'_i})$; then $k_i \equiv \bar{k}_i \pmod{d}$ and $k_i' = \bar{k}_i' \pmod{d}$. The condition that $T_1^{r_1}$ and $T_2^{r_2}$ are independent is that $\Delta = (\bar{k}_1 \bar{k}_2')$ is relatively prime to d. But

$$\Delta = \bar{\Delta} + d\ (\text{int. fcn. } \bar{k}_i, \bar{k}_i).$$

If, therefore, $[\bar{\Delta}, d] = 1$, $[\Delta, d] = 1$, and conversely. Q. E. D.

Corollary. *If* N_2 *is a divisor of* N_1, *the condition that* $T_1 = (\omega_{N_1}^{k_i})$ *and* $T_2 = (\omega_{N_2}^{k'_i})$ *are independent is*

$$[\Delta, N_2] = 1.$$

THEOREM II.—*Every group of ternary multiplicative substitutions with determinant* $+1$ *may be generated by at most two independent generators, and conversely, every Abelian group that can be generated by two generators is holoedrically isomorphic with a group of ternary multiplicative substitutions.*

First, let G be a group of order p^n, p a prime, and let

$$T_1 = (\omega_{p^{n_1}}^{k_i}) \qquad n_1 \not> n$$

be a substitution of maximum order in the group. If G is exhausted by the powers of T_1, the group is cyclic. If G contains yet other operations, let

$$T_3 = (\omega_{p^{n_2}}^{k'_i})$$

be a substitution of maximum order among the remaining elements which are independent of T_1. The group $\{T_1, T_2\}$ will then contain every ternary multiplicative substitution whose order is a divisor of p^{n_2}. For the conditions that

$$(T_1^{pn_2 - pn})^{\alpha}\, T_2^{\beta} = T = (\omega_{p^{n_2}}^{m_i}),$$

T arbitrary and of order p^{n_2} or less are

$$\left.\begin{aligned} \bar{k}_1\alpha + k'_1\beta &\equiv m_1, \\ \bar{k}_2\alpha + k'_2\beta &\equiv m_2, \end{aligned}\right\} \pmod{p^{n_2}}. \tag{7}$$

The congruences (7) have a solution whatever m_1 and m_2 may be since, by Theorem I, $[(k_1 k'_2), p^{n_2}] = 1$. There cannot then be a third independent generator.

The converse is easily shown to be true. For, let Γ be any Abelian group of order p^n with two independent generators. Its "Weber invariants"* are then p^n and p^{n_2} where $n_1 + n_2 = n$. Let

$$T_1 = (\omega_{p^{n_1}}^{A_i})$$

be any substitution of order p^{n_1}. It is possible to find a set of numbers B_i which, together with A_i, satisfy the conditions of Theorem I, and for which $\Sigma B_i \equiv 0 \pmod{p^{n_2}}$. Moreover, the notation may be chosen so that $n_1 \geqq n_2$.

To prove the theorem in the general case, let G_N be a ternary multiplicative group of order

$$N = p_1^{a_1} p_2^{a_2} \ldots . p_\lambda^{a_\lambda}, \qquad p_i \text{ a prime.}$$

---

* Weber, "Algebra," vol. II, §12.

Let $T_1^{(i)}$ and $T_2^{(i)}$ be the generators of the subgroup of order $p_i^{a_i}$ which exists in G_{N_1}. Further, let

$$G_{N_1} = \{ T_1^{(1)}, T_1^{(2)}, \ldots, T_1^{(\lambda)} \}$$

and

$$G_{N_2} = \{ T_2^{(1)}, T_2^{(2)}, \ldots, T_2^{(\lambda)} \},$$

whose orders are

$$N_1 = \prod_1^\lambda p_i^{n_1^{(i)}} \text{ and } N_2 = \prod_1^\lambda p_i^{n_2^{(i)}} \tag{8}$$

respectively. Moreover,

$$N_1 N_2 = N. \tag{9}$$

The orders of $T_1^{(i)}$ are relatively prime. Hence,

$$G_{N_1} = \{ T_1 \} \text{ where } T_1 = T_1^{(1)} . T_1^{(2)} \ldots . T_1^{(\lambda)}.*$$

Similarly,

$$G_{N_2} = \{ T_2 \} \text{ where } T_2 = T_2^{(1)} T_2^{(2)} T_2^{(3)} \ldots . T_2^{(\lambda)}.$$

If $n_1^{(i)} \gtreqless n_2^{(i)}$ for every i, $[N_1, N_2] = N_2$.

T_1 and T_2 are independent, for suppose $T_1^m = T_2^n$, m and n any positive integers; then

$$T_1^{\frac{mN_1}{p_i^{n_1^{(i)}}}} = T_2^{\frac{nN_1}{p^{n^{(i)}}}}$$

reduces to

$$T_1^{(i)p^{\frac{mN_1}{n_1^{(i)}}}} = T_2^{(i)p_i^{\frac{nN_1}{n_1^{(i)}}}},$$

Consequently m contains $p_i^{n_1^{(i)}}$ and n contains $p_i^{n_2^{(i)}}$. Therefore, m contains N_1 and n contains N_2. Conversely, let Γ_N be any Abelian group of order N which can be generated by two generators so that

$$\Gamma_N = \{ \theta_1, \theta_2 \}.$$

Among the Weber invariants of Γ_N, not more than two powers of any prime p_i can be found, viz. one which is a divisor of the order of θ_1 and the other a divisor of the order θ_2. But the Weber invariants of the most general group of ternary multiplicative substitutions are

$$p_1^{n_1^{(i)}}, p_1^{n_2^{(i)}}, p_2^{n_1^{(2)}}, p_2^{n_2^{(2)}} \ldots . p_\lambda^{n_1^{(\lambda)}}, p_\lambda^{n_2^{(\lambda)}},$$

---

* Weber, "Algebra," vol. II, §12.

and among the possible values of $n_1^{(i)}$ and $n_2^{(i)}$ may be found every bipartite partition of α_i, i. e. among the groups G_N will be found groups isomorphic with all possible Abelian groups that may be generated by two generators. Q. E. D.

§3.—*The Forms which remain Invariant with respect to the Substitutions of the Group* $\{T_1, T_2\}$.

Let $T_1 = (\omega_{N_1}^{k_i})$ and $T_2 = (\omega_{N_2}^{k_i'})$ be the generators of the group $\{T_1, T_2\}$ so chosen that $[N_1, N_2] = N_2$.

The invariant forms of $\{T_1, T_2\}$ are rational integral functions of monomial forms of the three types:

$$\left.\begin{array}{lll} \text{I.} & z_i^\alpha, & i = 1, 2, 3, \\ \text{II.} & z_i^\alpha z_j^\beta, & i, j = 1, 2, 3, \quad i \neq j, \\ \text{III.} & (z_1 z_2 z_3)^\alpha. & \end{array}\right\} \tag{10}$$

The conditions for the invariance of z_i^α are

$$\left.\begin{array}{l} k_i \alpha \equiv 0 \pmod{N_1}, \\ k_i' \alpha \equiv 0 \pmod{N_2}. \end{array}\right\} \tag{11}$$

By Theorem I, $[(k_i k_j'), N_2] = 1$. Hence,

$$\alpha \equiv 0 \pmod{N_2}.$$

Let
$$\alpha = \alpha_1 N_2,$$
and let
$$N_1 = N_2 \,.\, \bar{N}_1. \tag{12}$$
Also let $[k_i, \bar{N}] = q_i$; then

$$\alpha_1 \equiv 0 \mod \frac{\bar{N}}{q_i}. \tag{13}$$

The least value of α is therefore

$$\alpha = \alpha_1 \cdot \frac{\bar{N}}{q_i} = \frac{N_1}{q_i}. \tag{14}$$

The forms of type I are then given by

$$z_i^{\lambda \frac{N_1}{q_i}}, \qquad \lambda \text{ any positive integer.}$$

The conditions for the invariance of the form $z_i^\alpha z_j^\beta$ are

$$\left.\begin{array}{l} k_i\alpha + k_j\beta \equiv 0 \pmod{N_1}, \\ k_i'\alpha + k_j'\beta \equiv 0 \pmod{N_2}. \end{array}\right\} \tag{15}$$

Let $k_i k_j' - k_i' k_j \equiv \Delta$; then, since N_1 contains N_2,

$$\Delta\alpha \equiv 0 \pmod{N_2},$$
$$\Delta\beta \equiv 0 \pmod{N_2}.$$

But $[\Delta, N_2] = 1$, by Theorem I, so that

$$\alpha \equiv \beta \equiv 0 \pmod{N_2}.$$

The congruences (15) then reduce to the single congruence

$$k_i\alpha_1 + k_j\beta_1 \equiv 0 \pmod{\bar{N}}. \tag{16}$$

For $N_1 = N_2$ and consequently $\bar{N} = 1$, (16) has no meaning, but in this case the solution of (15) is

$$\alpha \equiv \beta \equiv 0 \pmod{N_1}.$$

For $\bar{N} > 1$, let $k_i = q_i k_i$, $i = 1, 2, 3$, where $q_i = [k_i, \bar{N}]$, and

$$\bar{N} = q_i q_j \bar{N}'. \tag{17}$$

From (16) it follows that α_1 contains q_j and β_1 contains q_i, so that (16) reduces to

$$k_i\alpha_2 + k_j\beta_2 \equiv 0 \pmod{\bar{N}'}, \tag{18}$$

where $\alpha_1 = q_j\alpha_2, \quad \beta_1 = q_i\beta_2.$

To solve (18), put

$$\alpha_2 = n \pmod{\bar{N}'},$$

then
$$k_i n + k_j\beta_2 \equiv 0 \mod \bar{N}'. \tag{19}$$

Let v be the least positive solution of the congruence

$$vk_j \equiv -k_i \pmod{\bar{N}'}. \tag{20}$$

From (19) and (20) it follows that

$$\beta_2 = nv \pmod{\bar{N}'}.$$

Let v_n be defined by

$$v_n \equiv nv \pmod{\bar{N}'}.$$

The general solution of (18) is then

$$\left.\begin{aligned}\alpha_2 &= n + \lambda\bar{N}',\\ \beta_2 &= v_n + \mu\bar{N}',\end{aligned}\right\}\lambda,\ \mu \text{ integers},$$

whence the solution of (15) is

$$\left.\begin{aligned}\alpha &= N_2 q_j(n + \lambda\bar{N}'),\\ \beta &= N_2 q_i(v_n + \mu\bar{N}').\end{aligned}\right\} \tag{21}$$

We have then the proposition:

THEOREM III.—*The invariant forms of the group* $\{T_1, T_2\}$ *are rationl integral functions of the following forms:*

$$\left.\begin{array}{lll} \text{I.} & z_i^{\frac{N_1}{q_i}} & i = 1, 2, 3. \\ \text{II.} & (z_i^{nq_j} z_j^{v_n q_i})^{N_2} & i, j = 1, 2, 3. \\ \text{III.} & z_1 z_2 z_3, & \end{array}\right\} \qquad (22)$$

where N_1 *and* N_2 *are the respective orders of* T_1 *and* T_2, $q_i = [k_i, N_1 \div N_2]$, *n is a positive integer* $< \frac{N_1}{N_2 q_i q_j}$ *and* v_n *is defined by the congruences*

$$k_j v + k_i \equiv 0 \left(\bmod \frac{N_1}{N_2 q_i q_j}\right), \qquad v_n \equiv nv \left(\bmod \frac{N_1}{N_2 q_i q_j}\right)$$

The full system* is easily found. The forms $z_i^{\frac{N_1}{q_i}}$ $i = 1, 2, 3$ and $z_1 z_2 z_3$ belong to the full system. It remains only to examine the forms

$$z_i^{nq_jN_2} z_j^{v_n q_i N_2} \qquad (23)$$

obtained by allowing n to run through the set of values 1, 2, ... $\bar{N}'-1$, where $\bar{N}'$ is defined by (17).

Recurring to the definition of $\bar{N}'$, it is seen that there are

$$\frac{\bar{N}}{q_1 q_2 q_3}(q_1 + q_2 + q_3) - 3$$

forms of the type (23). These forms, together with the four forms $z_i^{\frac{N_1}{q_i}}$ $i = 1, 2, 3$ and $z_1 z_2 z_3$ include the full system and, in some cases, coincide with it. This system of $\frac{\bar{N}}{q_1 q_2 q_3}(q_1 + q_2 + q_3) + 1$ forms is called the "reduced system."†

Suppose it be possible that for some partition of n for $n < \bar{N}'$,

$$\left.\begin{array}{l} n_1 + n_2 + \dots + n_\lambda = n \\ v_{n_1} + v_{n_2} + \dots + v_{n_\lambda} = v_n \end{array}\right\}, \quad n < \bar{N}' \qquad (24)$$

---

* The full system is defined to be a set of forms, the fewest possible in number, in terms of which every other form of the system is rationally expressible.

† See Professor Maschke's paper where the expression is used in a slightly different though strictly analogous sense.

hold simultaneously. It is evident that all forms $z_i^{nq_jN_2} z_j^{\nu_n q_i N_2}$, for which relations similar to (24) hold simultaneously, do not belong to the full system. It follows that the full system of the group $\{T_1, T_2\}$ consists of the forms $z_i^{\frac{N_1}{q_i}}$, $i = 1, 2, 3$, $z_1 z_2 z_3$ and those forms $z_i^{nq_jN_2} z_j^{\nu_n q_i N_2}$, for which the relations (24) are not simultaneously true.

§4.—*The Invariant Forms of the Group* $\{T_1, T_2, S\}$.

The group $\{T_1, T_2, S\}$, where S denotes the cyclic substitution $(z_1 z_2 z_3)$, is the most general ternary monomial group with determinant $+1$.

Since every invariant form is unchanged by S, the following types are admissible:

$$\left.\begin{array}{ll} \text{I.} & z_1^\alpha + z_2^\alpha + z_3^\alpha, \\ \text{II.} & z_1^\alpha z_2^\beta + z_2^\alpha z_3^\beta + z_3^\alpha z_1^\beta, \\ \text{III.} & z_1^\alpha z_2^\beta z_3^\gamma + z_2^\alpha z_3^\beta z_1^\gamma + z_3^\alpha z_1^\beta z_2^\gamma. \end{array}\right\} \tag{25}$$

If ρ be the least of the three integers α, β, γ in type III, the form is divisible by the invariant $(z_1 z_2 z_3)^\rho$, while the remaining factor is either of type I or of type II.

For I, we may write (z_1^α) and for II $(z_1^\alpha z_2^\beta)$. It follows directly that the forms which remain invariant with respect to the group $\{T_1, T_2, S\}$ are rational integral functions of $z_1 z_2 z_3$ and of forms of the types (z_1^α) and $(z_1^\alpha z_2^\beta)$.

The forms (z_1^α) go into $(\omega_{N_1}^{k_1\alpha} z_1^\alpha)$ by the substitution T_1, whence it follows that $\alpha \equiv 0 \pmod{N_1}$ is a necessary condition. This condition is also sufficient, since N_1 contains N_2. The invariant forms of the type (z_1^α) are then all given by $(z_1^{\lambda N_1})$, where λ is any positive integer.

The conditions that a term $z_i^\alpha z_j^\beta$ of $(z_1^\alpha z_2^\beta)$ shall be invariant are

$$\left.\begin{array}{l} k_i\alpha + k_j\beta \equiv 0 \pmod{N_1}, \\ k_i\alpha + k_j\beta \equiv 0 \pmod{N_2}, \end{array}\right\} \tag{26}$$

But these congruences are identical with (15) and consequently reduce to the single congruence

$$k_i\alpha_1 + k_j\beta_1 \equiv 0 \pmod{\bar{N}},$$

with notation the same as in §3. Giving to i and j all possible values, and remembering that $\Sigma k_i \equiv 0 \bmod \bar{N}$, we find

$$\left.\begin{array}{l} k_1\alpha_1 + k_2\beta_1 \equiv 0 \\ k_2\alpha_1 - (k_1 + k_2)\beta_1 \equiv 0 \end{array}\right\} \bmod \bar{N}. \tag{27}$$

Let $c=[k_1,\ k_2]$, and as before $q_i=[k_i,\ \bar{N}]$, then $[c,\ q_i]=1$ by reason of $\Sigma k_i \equiv 0 \pmod{N}$. Let $k_1=cx_1$, $k_2=cx_2$, then the congruences (26) show that

$$\alpha \equiv \beta \equiv 0 \pmod{q_1 q_2 q_3}.$$

Let

$$q_1 q_2 q_3 = Q, \quad \bar{N}=QR, \quad \alpha_1 = Q\alpha_2, \quad \beta_1 = Q_2\beta_2. \tag{28}$$

When the factors q_1, q_2, q_3 and c are divided out, (26) takes the form

$$\left.\begin{array}{l} x_1\alpha_2 + x_2\beta_2 \equiv 0 \\ x_2\alpha_2 - (x_1+x_2)\,\beta_2 \equiv 0 \end{array}\right\} \pmod{R}. \tag{29}$$

The coefficients of (28) are relatively prime to R. Let

$$\Delta = x_1^2 + x_1x_2 + x_2^2, \quad t=[\Delta,\ R], \quad \Delta = st, \quad R=rt. \tag{30}$$

It follows that α and β contain the factor r and the congruences (29) reduce to

$$\left.\begin{array}{l} k_1\alpha_3 + k_2\beta_3 \equiv 0\,, \\ k_2\alpha_3 - (k_1+k_2)\,\beta_3 \equiv 0\,, \end{array}\right\} \pmod{t}, \tag{31}$$

where

$$\alpha_2 = r\alpha_3, \quad \beta_2 = r\beta_3. \tag{32}$$

The first congruence of (31) is identical in form with (18). Its solution is therefore

$$\left.\begin{array}{l} \alpha_3 = n + \lambda t, \\ \beta_3 = v_n + \mu t, \\ vx_2 + x_1 \equiv 0 \pmod{t}, \\ v_n \equiv nv \pmod{t}. \end{array}\right\} \tag{33}$$

It is easy to show that this solution satisfies the second of (31). It is therefore the general solution of (31). Let

$$\vartheta = N_2\,Qr, \tag{34}$$

then, by reason of (27), (31) and (32), the solution of (26) is

$$\left.\begin{array}{l} \alpha = \vartheta\,(n + \lambda t), \\ \beta = \vartheta\,(v_n + \mu t), \\ vk_2 + k_1 \equiv 0 \pmod{t}, \\ v_n \equiv nv \pmod{t}, \end{array}\right\} \tag{35}$$

where $n = 0,\ 1,\ 2,\ \ldots.\ t-1$.

If the solution had been found by making $\beta_3 \equiv n \pmod{t}$, it would have taken the form

$$\left.\begin{aligned} \alpha &= \vartheta(w_n + \lambda' t), \\ \beta &= \vartheta(n + \mu' t), \\ w\varkappa_1 + \varkappa_2 &\equiv 0 \pmod{t}, \\ w_n &\equiv nw \pmod{t}. \end{aligned}\right\} \qquad (36)$$

The results obtained in the present section may be summed up as follows:

THEOREM IV.—*The invariant forms of the group* $\{T_1, T_2', S\}$ *are rational integral functions of the following forms;*

$$\left.\begin{aligned} &\text{I.} \quad (z_i^{N_1\lambda}),\ \lambda \text{ a positive integer.} \\ &\text{II.} \quad (z_1^{\vartheta(n+\lambda t)} z_2^{\vartheta(v_n+\mu t)}),\ \lambda,\ \mu \text{ positive integers.} \\ &\text{III.} \quad (z_1 z_2 z_3), \end{aligned}\right\} \qquad (37)$$

where the following definitions are to be observed: N_1 and N_2 are the orders of T_1 and T_2, $N_1 = N_2 \bar{N}$, $q_i = [k_i, \bar{N}]$, $\bar{N} = QR$,

$$t = [R, \varkappa_1^2 + \varkappa_1\varkappa_2 + \varkappa_2^2], \quad R = rt, \quad \vartheta = NrQ.^*$$

§5.—*The Quantities v, w and t.*

In the paper referred to above, Professor Maschke has given some relations between v, w and t which will be found useful in later investigations. The proofs, which are simple, will be found in Professor Maschke's paper.

1). $vw \equiv 1 \pmod{t}$. (38)

2). $v + w = t + 1$. (39)

3). v and w satisfy the congruence

$$x^2 - x + 1 \equiv 0 \pmod{t}. \qquad (40)$$

4). v and w are always distinct except for $t = 3$, in which case $v = w = 2$.

5). t as a number of the form

$$p_1^{\lambda_1} p_2^{\lambda_2} \ldots \quad \text{or} \quad 3p_1^{\lambda_1} p_2^{\lambda_2}, \qquad (41)$$

where p_i is a prime number of the form $3h + 1$. To these properties two others may be added.

---

* The solution of the congruences (26) occurs in a slightly different form in Professor Maschke's paper.

6). The solution of the congruence (40) is possible for those and only those numbers $t = 3^\delta p_1^{\lambda_1} p_2^{\lambda_2} \ldots\ldots, \delta = 0$ or 1.

For, since $[t, 4] = 1$, (40) is equivalent to

$$4x^2 - 4x + 4 \equiv 0 \pmod{t}$$

or

$$(2x+1)^2 + 3 \equiv 0 \pmod{t}.$$

Making $y = 2x + 1$, we have

$$y^2 + 3 \equiv 0 \pmod{t}.$$

If D be any number, the divisors of $y^2 - D$ are identical with the divisors of $z^2 - Du^2$.* The divisors of $z^2 + 3u^2$ are those and only those prime numbers of the form $3h + 1$.† From the existence of these solutions we may infer the existence of solutions of the form

$$t = 3^\delta p_1^{\lambda_1} p_2^{\lambda_2} \ldots\ldots, \ddagger$$
$$\delta = 0 \text{ or } 1.$$

7). Finally, for $t \equiv 0 \pmod{3}$,

$$[v - w, t] = 3$$

and for $t \not\equiv 0 \bmod 3$

$$[v - w, t] = 1.$$

For, from (38) and (39), one finds

$$(v - w)^2 + 3 \equiv 0 \pmod{t}. \tag{42}$$

6.—*The Full System for the Group* $\{T_1, T_2, S\}$.

If one makes in (37) the substitution $z_i^\vartheta = y_i$, the invariant forms of the group become rational integral functions of the forms

$$\text{I.}\quad (y_1^{kt}), \qquad \text{II.}\quad (y_1^{n+\lambda t} y_2^{v_n + \mu t}), \qquad \text{III.}\quad \sqrt[\vartheta]{y_1 y_2 y_3}. \tag{43}$$

The cases $t = 1$ and $t > 1$ are treated separately. For $t = 1$ the congruences (29) are satisfied by any positive integral values for α_3 and β_3. Since $\alpha = \vartheta\alpha_3$ and $\beta = \vartheta\beta_3$, the forms $(y_1^\alpha y_2^\beta)$ are invariant for every positive integral α and β. We have

$$(y_1^\alpha y_2^\beta) + (y_1^\beta y_2^\alpha) = S_1, \text{ a symmetric function};$$
$$(y_1^\alpha y_2^\beta) - (y_1^\beta y_2^\alpha) = S_2\Delta, \text{ an alternating function},$$

---

* Dirchlet-Dedekind, "Zahlentheorie," §52, ed. 1894. † Ibid. §70. ‡ Ibid. §35.

where S_2 is a symmetric function and Δ is the discriminant of $y_1 y_2 y_3$. We have then

$$(y_1^\alpha y_2^\beta) = \frac{S_1 + S_2\Delta}{2},$$

from which it follows immediately that the full system consists of the four forms

$$(y_1), \quad (y_1 y_2), \quad \sqrt[\vartheta]{y_1 y_2 y_3} \text{ and } \Delta. \tag{44}$$

Between these four forms there exists the relation

$$\Delta^2 = 18\,(y_1)\cdot(y_1 y_2)\cdot(y_1 y_2 y_3) - 4\,(y_1)^3\cdot y_1 y_2 y_3 - 4\,(y_1 y_2)^3 + (y_1 y_2)^2\cdot(y_1)^2 - 27\,(y_1 y_2 y_3)^3. \tag{45}$$

Case II. $t > 3$.

If ψ_n be defined by $\psi_n = (y_1^n y_2^{v_n})$, there are $t-1$ forms which are obtained by allowing n to run from 1 to $t-1$. Professor Maschke has proven the following theorem:

THEOREM V.—*If* $t > 1$, *every invariant form of the system* (43) *is expressible rationally in terms of the "reduced system," consisting of the* $t+1$ *forms* (y_1^t), $\sqrt[\vartheta]{y_1 y_2 y_3}$ *and* Ψ_n, $n = 1, 2, 3, \ldots\ t-1$.*

A general expression for the full system of such a reduced system has not been found, but in any given case the forms of the full system may be picked out by means of the following theorem:

THEOREM VI.—*The full system of the group* $\{T_1, T_2, S\}$, $t > 1$, *consists of the forms* (y_1^t), $\sqrt[\vartheta]{y_1 y_2 y_3}$ *and those forms* ψ_n *for which the relations*

$$n_1 + n_2 + \ldots = n, \; v_{n_1} + v_{n_2} + \ldots = v_n \qquad (n, n_i \overline{\lessgtr} t-1) \tag{46}$$

are not both true.

Let ψ_n be a ψ of minimum order in the set of ψ's for which the property in question is true. Then

$$\psi_{n_1}\psi_{n_2}\ldots - \psi_n + (\sqrt[\vartheta]{y_1 y_2 y_3})^\mu\,\Psi, \qquad \mu > 0, \tag{47}$$

where Ψ is a function of the forms ψ. According to hypothesis, the form Ψ cannot contain any ψ for which the property in question is true. Let $\psi_{n'}$ be another function of the set and of the next higher order, then

$$\psi_{n'} = \psi_{n'_1}\,\psi_{n_2}\ldots - A^{\mu'}\Psi',$$

* Maschke, loc. cit., p. 179.

Ψ cannot contain $\psi_{n'}$, and if it contains functions of the set ψ_n of lower degree they may be eliminated by a relation having the form (47). This process may be carried on so long as any of the ψ's having the property (47) remain. It is easy to show that it cannot be carried farther. Hence the theorem is true.

Cor. For $t > 3$ *the number of forms* ψ_n *belonging to the full system cannot exceed* $\frac{1}{2}(t-1)$ *when* $t \not\equiv 0$ *mod* 3 *or* $\frac{1}{2}(t-5)$ *when* $t \equiv 0$ (*mod* 3).

w may be taken less than v. If k be any positive integer such that

$$w + k \overline{\gtrless} t - 1,$$

then by (38),

$$v_{w+k} = v_w + v_k.$$

Consequently the number of ψ's belonging to the full system is less than w. But by (39),

$$v + w = t + 1.$$

Therefore, for $t > 3$,

$$w \overline{\gtrless} \tfrac{1}{2}(t-1).$$

For $t \equiv 0$ (mod 3) we have, by §5, 7),

$$v = w + 3m, \quad m \text{ a positive integer},$$

and

$$2w = t + 1 - 3m.$$

The least value of m is 2, whence,

$$w \overline{\gtrless} \tfrac{1}{2}(t-5).$$

CHAPTER II.

TERNARY MONOMIAL GROUPS WITH DETERMINANT ± 1.

§7.—*Groups of Ternary Multiplicative Substitutions with Determinant* ± 1.

In any ternary multiplicative group with determinant ± 1, those substitutions with determinant $+1$ form a subgroup with index 2. Let G_{2r} be a group with determinant ± 1 and G_r the subgroup with determinant $+1$. If the Weber invariants of G_r are

$$p_1^{n_1^{(1)}}, \quad p_1^{n_2^{(1)}}, \quad p_2^{n_1^{(2)}}, \quad p_2^{n_2^{(2)}} \cdots \cdot ,$$

the Weber invariants of G_{2r} are

$$2, \quad p_1^{n_1^{(1)}}, \quad p_1^{n_2^{(1)}}, \quad p_2^{n_1^{(2)}}, \quad p_2^{n_2^{(2)}} \cdots \cdot \qquad (48)$$

But if τ denote one of the substitutions

$$\tau_1 = (-1,\ 1,\ 1), \quad \tau_2 = (1,\ -1,\ 1), \quad \tau_3 = (1,\ 1,\ -1), \quad \tau_4 = (-1,\ -1,\ -1), \tag{49}$$

the Weber invariants of the group $\{T_1,\ T_2,\ \tau\}$ are precisely the numbers (48) We have then the proposition:

THEOREM VII.—*The most general ternary multiplicative group with determinant* ± 1 *is the group* $\{T_1,\ T_2,\ \tau\}$, *where* τ *is a substitution of order* 2 *and determinant* -1. *The Weber invariants of the group are*

$$2,\quad p_1^{n_1^{(1)}},\quad p_1^{n_1^{(2)}},\quad p_2^{n_2^{(1)}},\quad p_2^{n_2^{(2)}}\ \ldots\ldots, p_i \neq p_k. \tag{50}$$

Cor. If all the numbers p are odd primes, the group $\{T_1,\ T_2,\ \tau\}$ *is holoedrically isomorphic with one of the groups* $\{T_1,\ T_2\}$.

§8.—*The Invariant Forms of the Group* $\{T_1,\ T_2,\ \tau\}$.

By reason of the Corollary to Theorem VII only those groups $\{T_1,\ T_2,\ \tau\}$, for which N_1 and N_2 are both even, need be investigated. Let $p_1 = 2$. The group $\{T_1,\ T_2,\ \tau\}$ will then contain two independent substitutions T_1' and T_2' of orders $2^{n^{(1)}}$, $2^{n_1^{(2)}}$ respectively. Therefore, $T_1'^{2^{n_1^{(1)}}-1}$ and $T_2'^{2^{n_1^{(2)}}-1}$ are two of the substitutions

$$\sigma_1 = (1,\ -1,\ -1), \quad \sigma_2 = (-1,\ 1,\ -1), \quad \sigma_3 = (-1,\ -1,\ 1). \tag{51}$$

But $\sigma_i\sigma_j = \sigma_k$, $i, j, k = 1,\ 2,\ 3$ in some order, and

$$\tau_i\sigma_i = \tau_4, \quad \tau_4\sigma_i = \tau_i, \qquad i = 1,\ 2,\ 3,\ \ldots.$$

The group $\{T_1,\ T_2,\ \tau\}$ contains τ_1, τ_2, τ_3, τ_4 and the invariant forms are functions of z_1^2, z_2^2, z_3^2.

Let $N_1 = 2^{\lambda_1}Q_1$ and $N_2 = 2^{\lambda_2}Q_2$, $\lambda_2 \neq 0$ and $\overline{\gtrless}\lambda_1$, and $Q_1 \div Q_2 = \bar{Q}$, then $\bar{N} = 2^{\lambda_1-\lambda_2}\bar{Q}$ and $q_i = [k_i,\ \bar{N}]$ contains at most $2^{\lambda_1-\lambda_2}$. Therefore, $\dfrac{N_1}{q_i}$ contains 2^{λ_2} at least. It follows that all the forms (22) are invariant with respect to $\{T_1,\ T_2,\ \tau\}$ except z_1, z_2, z_3.

THEOREM VIII.—*The invariant forms of the group* $\{T_1,\ T_2,\ \tau\}$ *are rational integral functions of the forms*

$$\left.\begin{array}{lll} \text{I.} & z_i^{\frac{N_1}{q_i}} & i = 1,\ 2,\ 3. \\ \text{II.} & (z_i^{nq_j} z_j^{\nu_n q_i})^{N_2} & i, j = 1,\ 2,\ 3, \quad i \neq j. \\ \text{III.} & (z_1 z_2 z_3)^2. & \end{array}\right\} \tag{52}$$

The problem of finding the full system is the same as that in finding the full system for the group $\{T_1, T_2\}$ as may be seen by making $z_i^2 = y_i$, $i = 1, 2, 3$.

§9.—*The Invariant Forms of the Groups* $\{T_1, T_2, S, \tau\}$.

The invariant forms of the group $\{T_1, T_2, S\}$ were found to be

$$\left.\begin{array}{lll} (z_1^{N_1 k}), & (z_1^{(n+\lambda t)\vartheta} z_2^{(v_n+\mu t)\vartheta}), & (z_1 z_2 z_3)^\nu \\ (y_1^{kt}), & (y_1^{n+\lambda t} y_2^{v_n+\mu t}), & \sqrt[\vartheta]{(y_1 y_2 y_3)^\nu}. \end{array}\right\} \tag{37}$$

or (second line above)

To abbreviate the notation still further, let

$$H'_\kappa = (y_1^{\kappa t}), \quad \psi_{n,\lambda,\mu} = (y_1^{n+\lambda t} y_2^{v_n+\lambda t}) \text{ and } A = \sqrt[\vartheta]{y_1 y_2 y_3}. \tag{53}$$

$\psi_{n,\sigma,0}$ is then simply ψ_n, and the set of forms (37) takes the form

$$H_\kappa, \quad \psi_{n,\lambda,\mu}, \quad A^\nu, \tag{37a}$$

For the case N_1 even, since ϑ is even when N_1 is even, the set of forms is

$$H_\kappa, \quad \psi_{n,\lambda,\mu}, \quad A^{2\nu}. \tag{54}$$

For N_1 odd there are two subcases, viz. $\alpha)$ $\tau = \tau_4$; $\beta)$ $\tau \neq \tau_4$.

$\alpha)$ $\tau = \tau_4$. The invariant forms are

$$\left.\begin{array}{l} H_{2\kappa}, \quad \psi_{n,\lambda,\mu}, \quad n + v_n + \lambda + \mu \equiv 0 \pmod 2, \\ A^{2\nu}, \quad H_\kappa A^\rho, \quad \kappa \equiv \rho \equiv 1 \pmod 2, \\ \psi_{n,\lambda,\mu} A^\rho, \quad n + v_n + \lambda + \mu \equiv \rho \equiv 1 \pmod 2, \end{array}\right\} \tag{55}$$

$\beta)$ $\tau \neq \tau_4$. Since

$$S^{-1}\tau_1 S = \tau_2, \quad S^{-1}\tau_2 S = \tau_3, \quad S^{-1}\tau_3 S = \tau_1, \quad \tau_1\tau_2\tau_3 = \tau_4,$$

the invariant forms must be functions of z_1^2, z_2^2, z_3^2. They are therefore

$$H_\kappa, \quad \psi_{n,\lambda,\mu}, \quad A^\nu, \quad \kappa \equiv n + \lambda \equiv v_n + \mu \equiv \nu \equiv 0 \pmod 2. \tag{56}$$

It remains to find the full systems. For the case N_1 even, we know that H_κ and $\psi_{n,\lambda,\mu}$ are expressible rationally in terms of H_1, ψ_n and A^ϑ. It follows that the reduced system consists of the $t + 1$ forms,

$$H_1, \quad \psi_n, \qquad n = 1 \ldots\ldots t - 1 \text{ and } A^2. \tag{57}$$

For the case N_1 odd and $\tau = \tau_4$, we note that by Theorem V the set of forms (55) will be included in the system consisting of the following:

$$\left.\begin{array}{l}\text{1). The even forms } \psi_n. \\ \text{2). The products } \psi_{n_1} . \psi_{n_2} \text{ of two odd forms.} \\ \text{3). The products } H_1 . \psi_n \text{ where } \psi_n \text{ is an odd form.} \\ \text{4). The products } A . \psi_n, \ \psi_n \text{ odd.}\end{array}\right\} \tag{58}$$

To show that the form H_1^2 may he replaced by H_2, or vice versa, we have

$$\begin{aligned} H_1^2 &= H_2 + 2\,(y_1^t y_2^t) \\ &= H_2 + \text{Rat. fcn. } (\psi_n, \ A^\vartheta, \ A^\vartheta. \, H).^* \end{aligned}$$

That the reduction cannot be carried further in the general case is apparent from the case $t = 3$, since, for $t = 3$, all the forms (57) are found in the full system.† In most cases, however, it will happen that the system (57) admits of further reduction.

For the case N_1 odd and $\tau \neq \tau_4$ the invariant forms are the set (56) and these may be expressed in the form

$$H_\kappa(y^2), \quad \psi_{n,\lambda,\mu}(y^2), \quad A^\nu(y^2).$$

We find, for the even values of n, λ is even and

$$n + \lambda t = 2\,(n' + \lambda' t) \qquad n' = 1, \ 2, \ 3 \ \ldots . \ \frac{t-1}{2}.$$

and for odd values of n, λ is odd, so that

$$\begin{aligned} n + \lambda t &= 2\left(n'' + \frac{t+1}{2} + \lambda'' t\right), \quad n'' = 1, \ 2, \ 3 \ \ldots . \ \frac{t-3}{2} \\ &= 2\,(n''' + \lambda'' t), \quad n''' = \frac{t+1}{2}, \ \ \frac{t+3}{2} \ \ldots . \ t-1. \end{aligned}$$

And, moreover, by definition of v_n,

$$v_{2n} \equiv 2 v_n \ (\text{mod } t).$$

---

* Maschke, loc. cit., p. 176.

† Ibid., p. 180.

If one makes $y_i^2 = x_i$, the system (56) will take the form

$$H_\kappa(x), \quad \psi_{n,\lambda,\mu}(x), \quad A^\nu(x).$$

But these invariants are identical in form with the system (37). The full system is, therefore, found in the reduced system

$$H_1(x), \quad \psi_n(x), \quad A(x). \tag{59}$$

THEOREM IX.—*The form system of the group* $\{T_1, T_2, S, \tau\}$ *is*—

1) *for* N_1 *even,* H_κ, $\psi_{n,\lambda,\mu}$, $A^{2\nu}$; *the full system is found by replacing* A *by* A_2 *in the full system of the group* $\{T_1, T_2, S\}$;

2) *for* N_1 *odd and* $\tau = \tau_4$ *the form system is given by* (55) *and the full system is contained in the reduced system* (58);

3) *for* N_1 *odd and* $\tau \neq \tau_4$ *the form system is*

$$H_\kappa(y^2), \quad \psi_{n,\lambda,\mu}(y^2), \quad A^\nu(y^2),$$

and the full system is found by replacing y *by* y^2 *in the full system of* $\{T_1, T_2, S\}$.

§10.—*The Invariant Forms of the Group* $\{T_1, T_2, s\}$.

If i, j, l be the subscripts of the k's in $T = (\omega_{N_1}^{k_i})$ and if the transposition (i, l) be denoted by $s_{i,l}$, the invariant forms of the group $\{T_1, T_2, s_{i,l}\}$ are rational integral functions of the forms

$$z_j^\lambda, \quad z_i^\mu + z_l^\mu, \quad (z_i^\alpha + z_l^\alpha)\, z_j^\beta, \quad z_i^{\alpha'} z_j^{\beta'} + z_l^{\beta'} z_j^{\alpha'} \text{ and } z_1 z_2 z_3.$$

The exponent λ satisfies the congruences (11). It has been found to be

$$\lambda \equiv 0 \left(\text{mod}\, \frac{N_1}{q_j}\right). \tag{60}$$

The exponent μ satisfies the four congruences

$$\left.\begin{aligned} k_i\mu \equiv k_l\mu \equiv 0 \ (\text{mod}\ N_1), \\ k_i'\mu \equiv k_l'\mu \equiv 0 \ (\text{mod}\ N_2), \end{aligned}\right\}$$
$$\therefore\ \mu \equiv 0 \ (\text{mod}\ N_1), \tag{61}$$

since $[k_i, k_l, N_1] = 1$.

In order that the form $(z_i^\alpha + z_l^\alpha)\, z_j^\beta$ shall be invariant, α and β must satisfy

the congruences

$$\left.\begin{aligned} k_i\alpha + k_j\beta &\equiv 0 \pmod{N_1}, \\ k_l\alpha + k_j\beta &\equiv 0 \pmod{N_1}, \\ k'_i\alpha + k'_j\beta &\equiv 0 \pmod{N_2}, \\ k'_l\alpha + k'_j\beta &\equiv 0 \pmod{N_2}. \end{aligned}\right\} \tag{62}$$

It follows immediately that

$$\alpha \equiv \beta \equiv 0 \pmod{N_2},$$

whence the congruences (62) reduce to

$$\left.\begin{aligned} k_i\alpha_1 + k_j\beta_1 &\equiv 0 \pmod{\bar{N}}, \\ k_l\alpha_1 + k_j\beta_1 &\equiv 0 \pmod{\bar{N}}, \end{aligned}\right\} \tag{63}$$

where $\qquad \alpha_1 = \alpha_1 N_2 \beta \equiv \beta_2 N_2.$

As before, put $\bar{N} = q_1 q_2 q_3 R = QR$, where $q_i = [k_i, \bar{N}]$.

The congruences (63) then reduce to

$$\left.\begin{aligned} q_i \varkappa \alpha'_1 + \varkappa_j \beta'_1 &\equiv 0 \pmod{R}, \\ q_l \varkappa_l \alpha'_1 + \varkappa_j \beta'_1 &\equiv 0 \pmod{R}, \end{aligned}\right\} \tag{64}$$

where $\qquad \alpha_1 = \alpha'_1 Q, \quad \beta_1 = \beta'_1 q_i q_l, \quad k_i = q_i \varkappa_i.$

If either q_i or q_l contains a prime factor ε which is found in R, the same factor must occur in β'_1 and consequently in α'_1. When this factor is divided out, the resulting congruences will differ from (64) only in that the modulus will be $\frac{R}{l}$. If $\frac{R}{l}$ contains ε, this further factor is found in α and β also.

Let

$$Q_i = \frac{Q}{q_i} \qquad i = 1, 2, 3.$$

Also let P be the product of all the prime factors common to R and q_i and common to R and q_l, each one taken as often as it occurs in R, and let

$$\alpha_1 = \alpha_2 QP, \quad \beta_1 = \beta_2 Q_j P, \quad \bar{N} = QPR'. \tag{65}$$

The congruences (63) reduce to

$$\left.\begin{aligned} q_i \varkappa_i \alpha_2 + \varkappa_j \beta_2 &\equiv 0 \pmod{R'}, \\ q_l \varkappa_l \alpha_2 + \varkappa_j \beta_2 &\equiv 0 \pmod{R'}, \end{aligned}\right\} \tag{66}$$

in which the coefficients are prime to the modulus. To solve (66), let

$$t' = [k_i - k_l,\ R'],\quad k_i - k_l = s't' \text{ and } R' = r't'. \tag{67}$$

The congruences (66) will reduce to

$$\left.\begin{array}{l} k_i\alpha_3 + \varkappa_j\beta_3 \equiv 0 \pmod{t'}, \\ k_l\alpha_3 + \varkappa_j\beta_3 \equiv 0 \pmod{t'}, \end{array}\right\} \tag{68}$$

where $$\alpha_2 = \alpha_3 r',\quad \beta_2 = \beta_3 r'. \tag{69}$$

The solution of (68) is

$$\left.\begin{array}{lll} \alpha_2 & \equiv n & \pmod{t'}, \\ \beta_3 & \equiv v'_n & \pmod{t'}, \\ v'\varkappa_j + k_i & \equiv 0 & \pmod{t'}, \\ v'_n & \equiv nv' & \pmod{t'}. \end{array}\right\} \tag{70}$$

The solution of (62) is, therefore,

$$\left.\begin{array}{l} \alpha = N_2\, Q\, Pr'\,(n + \lambda t'), \\ \beta = N_2\, Q_j Pr'\,(v'_n + \mu t'), \end{array}\right\} \tag{71}$$
$$n = 0,\ 1,\ 2\ \ldots\ldots\ t' - 1.$$

In order that the forms $z_i^{\alpha'} z_l^{\beta'} + z_l^{\alpha'} z_i^{\beta'}$ may be invariant, the following congruences must be true:

$$\left.\begin{array}{l} k_i\alpha' + k_l\beta' \equiv k_l\alpha' + k_i\beta' \equiv 0 \pmod{N_1}, \\ k_i\alpha' + k'_l\beta' \equiv k'_l\alpha' + k'_i\beta' \equiv 0 \pmod{N_2}. \end{array}\right\} \tag{72}$$

These congruences reduce easily to

$$\left.\begin{array}{l} k_i\alpha'_2 + k_l\beta'_2 \equiv 0 \pmod{q_j R'}, \\ k_l\alpha'_2 + k_i\beta'_2 \equiv 0 \pmod{q_j R'}, \end{array}\right\} \tag{73}$$

where $$\alpha' = N_2\, Q_j\, P\alpha'_2,\quad \beta' = N_2\, Q_j\, P\beta'_2. \tag{74}$$

We know that $$q_j t' = [k_i^2 - k_l^2,\ \ q_j R'],$$

so that if $$\alpha'_2 = \alpha'_3 r',\quad \beta'_2 = \beta'_3 r', \tag{75}$$

we obtain $$\left.\begin{array}{l} k_i\alpha'_3 + k_l\beta'_3 \equiv 0 \pmod{q_j t'}, \\ k_l\alpha'_3 + k_i\beta'_3 \equiv 0 \pmod{q_j t'}. \end{array}\right\} \tag{76}$$

By processes similar to those already employed, we find for the solution of (72),

$$\left.\begin{array}{l} \alpha' = N_2\, Q_j\, Pr'\,(n \;+ \lambda q_j\, t'), \\ \beta' = N_2\, Q_j\, Pr'\,(v''_n + \mu q_j\, t'), \\ v'' k_l + k_i \equiv 0 \;(\text{mod}\; q_j\, t'), \\ v''_n \equiv n v'' \;(\text{mod}\; q_j\, t'), \\ n \;= 0,\ 1,\ 2 \,\ldots\ldots\, q_j\, t' - 1. \end{array}\right\} \qquad (78)$$

Let $\vartheta' = N_2\, Q_j\, P\gamma'$, $q_j\, t' = t''$, $z_i^{\vartheta'} = x_i$. We have then

THEOREM X.—*The invariant forms of the group* $\{T_1,\ T_2,\ S_{il}\}$ *are rational integral functions of*

$$\left.\begin{array}{l} x_j^{\kappa t'}, \quad \sqrt[\vartheta']{(x_1\, x_2\, x_3)^{\nu}}, \\ \left(x_i^{q_j(n' + \lambda t')} + x_l^{q_j\,(n' + \lambda t')}\right) x_j^{v'_{n'}} \\ \text{and} \quad x_i^{n'' + \lambda' t''}\, x_l^{v'_{n''} + \mu' t''} + x_i^{v'_{n''} + \mu' t''}\, x_l^{n'' + \lambda' t''}, \\ \textit{where } \kappa,\ \lambda,\ \nu,\ \lambda',\ \mu' \textit{ are positive integers.} \end{array}\right\} \qquad (79)$$

$v'_{n'}$ and $v''_{n''}$ *are defined by* (70) *and* (78) *and*

$$n' = 0,\ 1,\ 2 \,\ldots\ldots\, t',$$
$$n'' = 0,\ 1,\ 2 \,\ldots\ldots\, t''.$$

§11.—*The Quantities* v', v'' *and* t'.

The quantity v' is determined uniquely by either of the two congruences

$$\left.\begin{array}{l} v' k_j \equiv -\, k_i \;(\text{mod}\; t'), \\ v' k_j \equiv -\, k_l \;(\text{mod}\; t'). \end{array}\right\} \qquad (80)$$

With the aid of the relation $\Sigma k \equiv 0$ (mod t') one finds

$$2v' \equiv q_j \;(\text{mod}\; t'). \qquad (81)$$

If t' is odd, v' is determined uniquely by (81). If t' is even, v' is either

$$v'_0 \;\text{or}\; v'_0 + \frac{t'}{2}, \;\text{where}\; v'_0 \equiv \frac{q_j}{2} \left(\text{mod}\; \frac{t'}{2}\right). \qquad (82)$$

The quantity v'' is determined uniquely by the congruence

$$v'' k_l \equiv -\, k_i \;(\text{mod}\; q_j t'), \qquad (83)$$

We know that $$k_i^2 - k_l^2 \equiv 0 \pmod{q_j t'};$$

therefore, $$v''^2 - 1 \equiv 0 \pmod{q_j t'}. \tag{84}$$

The congruence (84) has at least one root for $q_j t' = 2$ and at least two roots for $q_j t' > 2$.*

From (84) we obtain easily

$$v'' + 1 \equiv 0 \pmod{t'} \tag{85}$$

and $$v'' - 1 \equiv 0 \pmod{q_j}. \tag{86}$$

From (85) and (86) it follows that $[q_j, t']$ is 1 or 2, while from (81), $(q_j, t') = 2$ when t' is even.

If, therefore, $[q_j, t] = 1$, v'' may be found from (86) and (87). It is

where $$\left.\begin{aligned} v'' &= 1 + q_j \rho, \\ q_j\rho + 2 &\equiv 0 \pmod{t'}, \end{aligned}\right\} \tag{87}$$

If, however, $[q_j, t] = 2$, then v'' is one of the two numbers

$$1 + q_j\rho_0, \quad 1 + q_j\left(\rho_0 + \frac{t'}{2}\right),$$

where q_j is the smaller of the two roots of $q_j \rho + 2 \equiv 0 \pmod{t'}$, unless $t' = 2$.†
For $t' = 2$, (86) gives at once

$$v'' = 1.$$

These results may be stated as follows:

For t' odd, v' and v'' are given by (81) *and* (87). *For t' even and* >2, *v' is one of the numbers v'_0 or $v'_0 + \frac{t'}{2}$, where* $v'_0 \equiv \frac{q_j}{2}\left(\text{mod}\ \frac{t'}{2}\right)$, *and v'' is one* numbers $1 + q_j\rho_0$, $1 + q_j\left(\rho_0 + \frac{t'}{2}\right)$, *where ρ_0 is the smaller of the roots of* $q_j\rho + 2 \equiv 0 \pmod{t'}$. *For* $t' = 2$, $v'' = 1$.

---

* Dirichlet, "Zahlentheorie," p. 88, ed. 1894.

† Serret, "Alg. Sup.", No. 292.

§12.—*The Full System of the Group* $\{T_1, T_2, S\}$.

For brevity let

$$\left.\begin{aligned} A' &= \sqrt[\vartheta']{(x_1 x_2 x_3)}. \\ \phi_{n,\lambda,\mu} &= x_i^{n+\lambda t''} x_l^{v'_n + \mu t''} + x_i^{v'_n + \mu t''} x_l^{n+\lambda t''}, \\ \chi_{n,\lambda} &= \left(x_i^{q_j(n+\lambda t')} + x_l^{q_j(n+\lambda t')}\right) x_j^{v'_n}. \end{aligned}\right\} \tag{88}$$

ϕ_n and χ_n will be written for $\phi_{n,0,0}$ and $\chi_{n,0}$, and where no ambiguity can arise, $\phi_{n,\lambda}$ and $\phi_{n,\mu}$ will be written for $\phi_{n,\lambda,0}$ and $\phi_{n,0,\mu}$.

The problem is then to find the full system for the set of forms

$$x_j^{\kappa t}, \quad A'^{\nu}, \quad \phi_{n,\lambda,\mu} \text{ and } \chi_{n,\lambda}.$$

$x_j^{t'}$ and A' evidently belong to the full system.

1). The form $x_i^{t'} x_l^{t'}$ is invariant, since $(x_i x_j x_l)^{t'}$ and $x_j^{t'}$ are both invariant. It is easily shown that $\phi_{t'} = 2x_i^{t'} x_l^{t'}$.

2). The forms $\chi_{n,\lambda}$ are expressible in terms of the forms $x_j^{t'}$, ϕ_n, $n = 1, 2, 3 \ldots\ldots t'' - 1$, χ_n, $n = 1, 2, 3 \ldots\ldots t' - 1$ and the form $\chi_{0,1} = x_i^{t''} + x_l^{t''}$. For we have

$$\chi_{0,1} \cdot \chi_{n,\nu} = \chi_{n,\nu+1} + \tfrac{1}{2}\phi_{t'}^{q_j} \cdot \chi_{n,\nu-1},$$

whence

$$\chi_{n,\nu+1} = \chi_{0,1} \cdot \chi_{n,\nu} - \tfrac{1}{2}\phi_{t'}^{q_j} \cdot \chi_{n,\nu-1}.$$

If, therefore, the proposition is true for $\lambda \leqq \nu$, it is true for $\lambda = \nu + 1$. But it is true for $\lambda = 1$ since, by multiplication,

$$\chi_{0,1} \cdot \chi_n = \chi_{n,1} + \left(x_i^{q_j t'} x_l^{q_j n} + x_l^{q t'} x_i^{q_j n}\right) x^{v'_n}.$$

If $q_j n > v'_n$, the last term contains the invariant factor $(x_1 x_2 x_3)^{v'_n}$ and the other factor is one of the set ϕ_n. If $q_j n < v'_n$, the factors of the last term are the invariant $(x_1 x_2 x_3)^{q_j n}$ and one of the set χ_n.

The case $q_j n = v_n$ cannot occur since, in such case,

$$\begin{aligned} q_j n - v'_n &\equiv n'(q_j - v')(\text{mod } t') \\ &\equiv nv' \ (\text{mod } t') \text{ by } (81) \\ &\equiv 0 \ (\text{mod } t'). \end{aligned}$$

But, by definition, $[v' . t''] = 1$; then $nv' \equiv 0$ (mod t') gives $n \equiv 0$ (mod t'), which case is excluded.

The proposition is thus proven for all values of λ.

3). The forms $\phi_{n, \lambda, \mu}$ are expressible in terms of the forms

$$x_i^{t''} x_l^{t'}, \quad \chi_{0,1}, \quad \phi_{n,1,0} \text{ and } \phi_{v_n'',1,0}.$$

The proposition is evident for $\phi_{n, \lambda, \lambda}$. To fix the ideas, let $\lambda > \mu$, then, after the invariant factor $(x_i^{t''} x_l^{t''})^{\mu}$ is removed, it remains to consider the factor $\phi_{n, \lambda'}$, $\lambda' = \lambda - \mu$. One finds

$$\phi_{n, \nu} \cdot \chi_{0,1} = \phi_{n, \nu+1} + x_i^{t''} x_l^{t''} \cdot \phi_{n, \nu-1},$$

so that the assertion is true for $\lambda = \nu + 1$ if it is true for $\lambda \overline{\gtrless} \nu$. It is true for $\lambda = 1$; hence true universally.

Similar considerations hold for the forms $\phi_{v_n'', \mu}$.

4). The forms $\phi_{n,1,0}$ and $\phi_{v_n'',1,0}$ are expressible in terms of $x_i^{t'} x_l^{t'}$, $\chi_{0,1}$ and the forms ϕ_n.

If one of these two forms is known, the other is known from the relation

$$\phi_n \cdot \chi_{0,1} = \phi_{n,1,0} + \phi_{v_n'',1,0}.$$

Let us consider the forms $\phi_{v_n'',1,0}$.

α). If $n = t'$, $v''_n = t'$, and $\phi_{v_n'',1,0}$ breaks up into the two known forms $x_i^{t''} x_j^{t''}$ and $\chi_{0,1}$.

β). If $n > t'$, we may suppose that $\rho t' < n < (\rho + 1) t'$. Then

$$\phi_{v_n'',1,0} = (x_i^{t'} x_l^{t'})^{\rho} (x_i^{n-\rho t'} x_l^{v_n''+t''-nt'} + x_i^{v_n''+t''-\rho t} x_l^{n-\rho t'}). \tag{89}$$

When $v_n'' - \rho t' < 0$, the second factor on the right of (88) is one of the forms ϕ_n. If, however, $v_n'' - \rho t' > 0$, we have

$$\begin{aligned} v_n'' - \rho t' &\equiv (n - \rho t') v'' \pmod{t''} \quad \text{by (86)} \\ &\equiv v''_{n-\rho t'} \pmod{t''}. \end{aligned}$$

For the case under discussion

$$v_n'' - \rho t' = v''_{n-\rho t'}.$$

We have then

$$\phi_{v_n'',1,0} = (x_i^{t'} x_l^{t'}) \, \phi_{v_n''-\rho t',1}.$$

The determination of the forms $\phi_{v_n'',1}$ is then made to depend upon the solution of the next case, viz.

γ). $n < t'$.

If $v''_n > t'$, we have at once

$$\phi_n \cdot \chi_{0,1} = (x_i^{t'} x_l^{t'})^\rho \phi_{n+t''-\rho t'} + \phi_{v''_n, 1, 0}.$$

If both n and v''_n are less than t', $\phi_n = \phi_{v''_n}$ is of degree t', since $n + v'_n \equiv n(v+1) (\text{mod } t'')$ is divisible by t' by (84). Moreover, n and v''_n are different for all values of n when t' is odd, and for all values except $n = \frac{t'}{2}$ when t' is even, since, if $n = v''_n$, we have

$$n(1 - v) \equiv 0 \ (\text{mod } q_j t').$$

If t' is odd, $1 - v''$ contains q_j and no other factor of the modulus. If t' is event $1 - v''$ contains q_j and 2 by (85) and (86).

$\therefore n = t'$ or $\frac{t'}{2}$, according as t' is odd or even. The corresponding form is $(x_i x_l)^{t'}$ or $(x_i x_l)^{\frac{t'}{2}}$. Consequently the form $\phi_{n,1}$ breaks up into the two known factors

$$(x_i x_l)^{t'} \text{ and } \chi_{0,1} \text{ or } (x_i x_l)^{\frac{t'}{2}} \text{ and } \chi_{0,1}.$$

If $n \neq v''_n$, $\phi_{n,1}$ is identical with some $\phi_{v''_n, 1}$ when n and v'' are both less than t', so that we need consider only the cases where $n > v''_n$.

It may be shown that

$$\phi_n \cdot \phi_{n - v''_n} = \phi_{v''_n, 1} + x_i^{2n - v''_n} x_l^{2v''_n - n + t''} + x_l^{2n - v''_n} x_i^{2v''_n - n + t''}. \tag{90}$$

If $2v''_n - n'' < 0$, the problem is solved, but if $2v''_n - n > 0$, (90) may be written

$$\phi_n \cdot \phi_{n - v''_n} = \phi_{v''_n, 1} + \phi_{v''_{n_1}, 1}, \tag{91}$$

where it may be shown that $v''_{n_1} > v''_n$, and consequently $< n$ and

$$n_1 = 2v''_n - n \not> n.$$

The proof may be completed by induction.

5). The forms ϕ_n are expressible in terms of the first t' forms of the set.

For any $n > t'$, one may write $n = n_1 + \lambda t'$, $n_1 < t'$. Then

$$v''_n \equiv v''_{n_1} + \lambda t' \ (\text{mod } t'').$$

It follows directly that for $n > t'$,

$$\Phi_n = (x_i x_l)^{\lambda t'} \cdot \Phi_{n_1},$$

so that 5) is proven.

The lemmas 1), 2), 3), 4), 5) give the following theorem:

THEOREM XI.—*The invariant forms of the group* $\{T_1, T_2, s_{i,k}\}$ *are expressible rationally in terms of the* $2(t'+1)$ *forms*

$$\left.\begin{array}{l} x_j^{t'},\ \sqrt[\vartheta']{x_1 x_2 x_3}, \\ \chi_n = (x_i^{q_j n} + x_l^{q_j n})\, x_j^{v'_n}, \qquad \Phi_n = x_i^n x_l^{v''_n} + x_l^n x_i^{v''_n}, \\ \qquad\qquad n = 1, 2, 3 - t', \end{array}\right\} \tag{92}$$

where t', v'_n, v''_n, ϑ' *and* q_j *have the meanings assigned in* §10, *and* $x_i = z_i^{\vartheta'}$. *The full system will consist of the forms* $x_j^{t'}$, $x_i^{t''} + x_l^{t''}$, *the forms* χ_n, *for which* $n_1 + n_2 = n$ *and* $v'_{n_1} + x'_{n_2} = n$, *are not both true and the forms* Φ_n, *for which* $n \overline{\gtrless} t'$, *and* $n_1 + n_2 = n$ *and* $v''_{n_1} + v''_{n_2} = v''_n$ *are not both true.*

§13.—*The Invariant Forms of the Group* $\{T_1, T_2, s_{ik}, \tau\}$.

The invariant forms of the group $\{T_1, T_2, S_{ik}, \tau\}$ are all found among the forms of the group $\{T_1, T_2, s_{ik}\}$. It is clear moreover that τ either leaves any given invariant of the latter group unchanged or simply changes its sign. The invariant forms of the group $\{T_1, T_2, s_{ik}, \tau\}$ will then be found by imposing proper conditions upon the exponents $\varkappa$, λ, μ, λ', μ', ν of the forms (79) and adding to the forms thus obtained certain products of forms which change sign with respect to τ.

There are several cases with subcases depending upon the character of ϑ', t', q_j and t''. The results are here given without proof.

Case I. ϑ' even.

The form system is the system obtained from (92) by excluding odd powers of $\sqrt[\vartheta']{x_1 x_2 x_3}$, and in the full system $\sqrt[\vartheta']{x_1 x_2 x_3}$ is replaced by $\sqrt[\vartheta']{(x_1 x_2 x_3)^2}$.

Case II. ϑ' odd, $t'' = q_j t'$ even.

There are several subcases depending on the character of t' and q_j and the particular τ* that enters into the group.

* See §7 (49), above.

1). t' even.

1a). $\tau = \tau_j$ or τ_4.

In the forms $\chi_{n,\lambda}$, n must be even and the remaining condition to be imposed upon the exponents of (79) is $\nu \equiv 0 \pmod 2$. Besides the forms thus obtained, one has also to include the forms

$$\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \chi_{n,\lambda}, \quad \chi_{n'\lambda}, \cdot \chi_{n'',\lambda}, \quad n,\ n' \text{ and } n'' \text{ odd.}$$

There is a reduced system consisting of the forms

$$x_j^{t'}, \quad \sqrt[\vartheta']{x_1 x_2 x_3}, \quad \phi_n, \quad (n = 1, 2, 3 \ldots\ldots t'), \quad \chi_{2n}, \quad n = 1, 2 \ldots\ldots \frac{t'}{2},$$

$$\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \chi_{2n-1} \quad n = 1, 2 \ldots\ldots \frac{t'}{2}, \quad \chi_{n_1} \cdot \chi_{n_2}, \quad n_1 \text{ and } n_2 \text{ both odd.}$$

1b). $\tau = \tau_i$ or τ_l.

n must be even in the forms $\phi_{n,\lambda,\mu}$ and we must have also $\nu \equiv 0 \pmod 2$.

The forms $\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \phi_{n,\lambda,\mu}$, n odd and $\phi_{n'\lambda,\mu} \cdot \phi_{n'',\lambda,\mu}$, n' and n'' both odd, are to be included.

For a reduced system, we have

$$x_j^{t'}, \quad \phi_{2n}, \quad n = 1, 2, 3 \ldots\ldots \frac{t'}{2}, \quad \chi_n, \quad n = 1, 2 \ldots\ldots t',$$

$$\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \phi_{2n-1}, \quad n = 1, 2 \ldots\ldots \frac{t'}{2}, \quad \phi_{n'} \cdot \phi_{n''}, \quad n' \text{ and } n'' \text{ both odd.}$$

2). t' odd, q_j even.

2a). $\tau = \tau_j$ or τ_4.

The conditions to be imposed upon the exponents are $\varkappa \equiv \rho \equiv v'_n \equiv 0 \pmod 2$. The forms

$$x_j^{t'} \cdot \chi_{n,\lambda}, \quad \sqrt[\vartheta']{x_1 x_2 x_3} \cdot \chi_{n,\lambda}, \quad v'_n \text{ odd}, \quad \chi_{n',\lambda} \cdot \chi_{n'',\lambda},$$

n' and n'' both odd, are to be included.

There is a reduced system consisting of the forms

$$x_j^{2t'}, \quad \sqrt[\vartheta']{(x_1 x_2 x_3)^2}, \quad \phi_n, \quad n = 1, 2, 3 \ldots\ldots t', \quad \chi_n, \quad v'_n \text{ even},$$
$$x_j^{t'} \cdot \chi_n \text{ and } \sqrt[\vartheta']{x_1 x_2 x_3} \cdot \chi_n, \quad v'_n \text{ odd},$$
$$\chi_{n'} \cdot \chi_{n''}, \quad n' \text{ and } n'' \text{ both odd.}$$

2b). $\tau = \tau_i$ or τ_l.

The form-system is identical with that in the case 1b) above.

Case III. ϑ' odd and t'' odd.

1). $\tau = \tau_j$.

The form-system is identical with that of the case 1a) under II.

2). $\tau = \tau_4$.

The conditions are

$$\varkappa \equiv \nu \equiv n + v'_n + \lambda \equiv n + v''_n + \lambda + \mu \equiv 0 \pmod 2.$$

To the forms thus obtained must be added the forms

$x_j^{t'} \cdot \sqrt[\vartheta']{x_1 x_2 x_3}$, $x_j^{t'} \cdot \phi_{n,\lambda,\mu}$, $x_j^{t'} \cdot \chi_{n,\lambda}$, $\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \chi_{n,\lambda}$, $\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \phi_{n,\lambda,\mu}$, $\phi_{n,\lambda,\mu} \cdot \chi_{n,\lambda}$, $\phi_{n',\lambda,\mu} \cdot \phi_{n'',\lambda,\mu}$, $\chi_{n',\lambda} \cdot \chi_{n'',\lambda}$,

for which the conditions $n + v'_n + \lambda \equiv n + v''_n + \lambda + \mu \equiv 1 \pmod 2$ hold. There exists a reduced system consisting of the forms

$$x_j^{2t'}, \quad \sqrt[\vartheta']{(x_1 x_2 x_3)^2}, \quad \chi_n, \quad n + v'_n \text{ even}, \quad \phi_n, \quad n + v''_n \text{ even},$$

together with the product made up by taking two distinct factors from the forms

$$x_j^{t'}, \quad \sqrt[\vartheta']{x_1 x_2 x_3}, \quad \chi_n, \ n + v'_n \text{ odd and } \phi_n, \ n + v''_n \text{ odd}.$$

3). $\tau = \tau_i$ or τ_l.

The conditions are

$$\varkappa \equiv \nu \equiv n' + \lambda \equiv n'' + \lambda \equiv v''_{n''} + \mu \equiv 0 \pmod 2,$$

where n' and n'' belong to $\chi_{n,\lambda}$ and $\phi_{n,\lambda,\mu}$ respectively.

To these forms must be added the forms $x_j^{t'} \cdot \sqrt[\vartheta']{x_1 x_2 x_3}$, together with $x_j^{t'} \cdot \chi_{\mu,\lambda}$, $x_j^{t'} \cdot \phi_{n,\lambda,\mu}$, $\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \chi_{n,\lambda}$, $\sqrt[\vartheta']{x_1 x_2 x_3} \cdot \phi_{n,\lambda,\mu}$, $\chi_{n',\lambda,} \cdot \chi_{n'',\lambda}$, $\phi_{n',\lambda,\mu} \cdot \phi_{n'',\lambda,\mu}$ and $\chi_{n,\lambda} \cdot \phi_{n,\lambda,\mu}$, for which

$$n' + \lambda \equiv n'' + \lambda \equiv v''_{n''} + \mu \equiv 1 \pmod 2.$$

There is a reduced system consisting of the following forms:

$$x_j^{2t'}, \ \sqrt[\vartheta']{(x_1 x_2 x_3)^2}, \ \chi_n \ n \text{ even}, \ \phi_n, \ n \text{ and } v''_n \text{ even},$$

together with the products taken two at a time of the forms x_j^t, $\sqrt[\vartheta']{x_1 x_2 x_3}$, χ_n n odd, ϕ_n, n and v''_n not both even.

§14.—*The Invariant Forms of the Group* $\{T_1, T_2, S, s\}$.

If S and s be the generators of the symmetric group of three elements, the invariant forms of the group $\{T_1, T_2, S, s\}$ are rational integral functions of the symmetric functions

$$\Sigma z^\kappa, \quad \Sigma z_1^\alpha z_2^\beta, \quad (z_1 z_2 z_3)^\nu.$$

The exponent ν is any integer, while $\kappa \equiv 0 \pmod{N_1}$.

The conditions that the form $\Sigma z_1^\alpha z_2^\beta$ shall be invariant are given by six congruences of the form

$$k_i \alpha + k_j \beta \equiv 0 \pmod{N_1} \tag{93}$$

and six of the form

$$k_i' \alpha + k_j' \beta \equiv 0 \pmod{N_2}, \tag{94}$$

in which the numbers i and j are any arrangement of two of the numbers 1, 2, 3.

From the two congruences

$$k_i \alpha + k_j \beta \equiv 0 \pmod{N_2}$$

and

$$k_i' \alpha + k_j' \beta \equiv 0 \pmod{N_2},$$

one finds

$$\alpha \equiv 0 \pmod{N_2}, \quad \beta \equiv 0 \pmod{N_2}.$$

Let

$$\alpha = N_2 \alpha_1, \quad \beta = N_2 \beta_1, \tag{95}$$

then the twelve congruences (93) and (94) reduce to six of the form

$$k_i \alpha_1 + k_j \beta_1 \equiv 0 \pmod{\bar{N}}. \tag{96}$$

By reason of the relation $\Sigma k \equiv 0 \pmod{N_1}$, the six congruences (96) reduce to four, which may be written as follows:

$$\left.\begin{aligned} k_1 \alpha_1 + k_2 \beta_1 &\equiv 0 \pmod{\bar{N}}, \\ k_2 \alpha_1 - (k_1 + k_2) \beta_1 &\equiv 0 \pmod{\bar{N}}, \end{aligned}\right\} \tag{97}$$

$$\left.\begin{aligned} k_2 \alpha_1 + k_1 \beta_1 &\equiv 0 \pmod{\bar{N}}, \\ (k_1 + k_2) \alpha_1 + k_2 \beta_1 &\equiv 0 \pmod{\bar{N}}. \end{aligned}\right\} \tag{98}$$

in which the notation is identical with that in the congruences (27).

Comparing (97) and (98) with (27), one has at once the solutions sought, viz. For (97),

$$\left.\begin{array}{ll}\left.\begin{array}{l}\alpha = N_2\,Qr\,(n \;\;+\lambda t)\,,\\ \beta = N_2\,Qr\,(v_n \;+\mu t)\end{array}\right\}\text{(a)}\\ \text{or}\quad \left.\begin{array}{l}\alpha = N_2\,Qr\,(w_n + \lambda' t)\,,\\ \beta = N_2\,Qr\,(n \;+\mu' t)\,,\end{array}\right\}\text{(b)}\\ \text{and for (98),}\\ \left.\begin{array}{l}\alpha = N_2\,Qr\,(v_n \;+\lambda t)\,,\\ \beta = N_2\,Qr\,(n \;+\mu t)\,,\end{array}\right\}\text{(c)}\\ \text{or}\quad \left.\begin{array}{l}\alpha = N_2\,Qr\,(n \;+\lambda' t)\,,\\ \beta = N_2\,Qr\,(w_n + \mu' t)\,.\end{array}\right\}\text{(d)}\end{array}\right\}\qquad (99)$$

If one compares (a) and (d) or (b) and (c) of (99) the following condition is obtained for n, viz.

$$n\,(v - w) \equiv 0 \pmod{t'}. \qquad (100)$$

Two cases arise:

Case I. $[(v - w)\,,\, t] = 1$.

The congruence (100) has no solution except $n \equiv 0 \pmod{t}$, and, consequently, (93) and (94) have no solution except

$$\alpha \equiv \beta \equiv 0 \pmod{N_1},$$

The invariant forms are then symmetric functions of $z_1^{N_1}$, $z_2^{N_1}$, $z_3^{N_1}$, together with powers of $z_1 z_2 z_3$. The full system is

$$\Sigma z_1^{N_1}, \quad \Sigma z_1^{N_1} z_2^{N_1}, \quad z_1 z_2 z_3\,. \qquad (101)$$

Case II. $[v - w\,,\, t] \neq 1$.

It was shown in §§5, 7, that if $[(v - w)\,,\, t] \neq 1$, then $[(v - w)\,,\, t] = 3$. If $v - w = 3m$ and $t = 3s$ one finds

$$n \equiv 0 \pmod{s}.$$

Let

$$n = n_1\, s\,;$$

then since

$$v_n = v_{n_1 s} \equiv n_1 s v \pmod{3s},$$

$v_{n_1 s}$ is divisible by s.

Let

$$\frac{v_{n_1 s}}{s} = \bar{v}_{n_1},$$

We find $$\bar{v}_{n_1} \equiv n_1 v \pmod 3.$$

It follows immediately that the solutions which satisfy the twelve congruences (93) and (94), are of the form

$$\left.\begin{aligned} \alpha &= \vartheta''(n + 3\lambda), \\ \beta &= \vartheta''(\bar{v}_n + 3\mu), \end{aligned}\right\} n = 0, 1, 2, \tag{102}$$

when $\vartheta'' = N_2\, Qrs = \vartheta s = \dfrac{N_1}{3}$.

Let $z_i^{\vartheta''} = \xi_i$. The invariant forms sought are then

$$\Sigma\xi_1^{3\kappa}, \quad \Sigma\xi_1^{n+3\lambda}\,\Sigma\xi_2^{\bar{v}_n+3\mu}, \quad (\xi_1\,\xi_2\,\xi_2)^{\frac{3\nu}{N_1}} \tag{103}$$

where $n = 0, 1, 2$, and $\varkappa, \lambda, \mu, \nu$ are arbitrary integers.

Furthermore, the congruence

$$x^2 - x + 1 \equiv 0 \pmod t,$$

of which v is a root, may be written in the present case

$$(2x - 1)^2 + 3 \equiv 0 \pmod{3s}.$$

It follows that $$2v - 1 \equiv 0 \pmod 3$$

and that $$v \equiv 2 \pmod 3.$$

Evidently $v_1 = 2$ and $v_2 = 1$.

The set of forms $\Sigma\xi_1^{1+3\lambda}\,\xi_2^{2+3\mu}$ is identical with the set $\Sigma\xi_1^{2+3\lambda}\,\xi_2^{1+3\mu}$. We may then write the forms (103) as follows:

$$\Sigma\xi_1^{3\kappa}, \quad \Sigma\xi_1^{n+3\lambda}\,\xi_2^{2n+3\mu}, \quad (\xi_1\,\xi_2\,\xi_3)^{\frac{3\nu}{N}}, \qquad n = 0, 1. \tag{104}$$

The results may be summed up in the following:

THEOREM XII.—*If* $t \not\equiv 0 \pmod 3$, *the invariant forms of the group* $\{T_1, T_2, S, s\}$ *are given by*

$$\Sigma\xi_1^{3\kappa}, \quad \Sigma\xi_1^{3\lambda}\,\xi_2^{3\mu}, \quad \sqrt[N_1]{(\xi_1\,\xi_2\,\xi_3)^{3\nu}}.$$

If $t \equiv 0 \pmod 3$, *they are given by*

$$\Sigma\xi_1^{3\kappa}, \quad \Sigma\xi_1^{n+3\lambda}\,\xi_2^{2n+3\mu}, \quad (n = 0, 1), \quad \sqrt[N_1]{(\xi_1\,\xi_2\,\xi_3)^{3\nu}}.$$

It remains to find the full system of the system (104). Let

$$\Sigma\xi_1^3 = C_1, \quad \Sigma\xi_1^3\,\xi_5^3 = C_2, \quad (\xi_1\,\xi_2\,\xi_3)^3 = C_3, \quad \Sigma\xi_1\,\xi_2^2 = D. \tag{105}$$

We have only to examine the forms $\Sigma\xi_1^{1+3\lambda}\xi_2^{2+3\mu}$, since all other forms of the system are expressible in terms of C_1, C_2, $C_3^{\frac{1}{N_1}}$. Let $\Sigma\xi_1^{1+3\lambda}\xi_2^{2+3\mu} = D_{\lambda,\mu}$. The forms $D_{\lambda,\mu}$ are expressible rationally in terms of C_1, C_2, C_3 and D. For, suppose the statement be true for all forms of order $3n$ in the ξ's or less; then the $n+1$ relations

$$\begin{aligned} \Sigma\xi_1^6 . D &= D_{3,n-1} + D_{0,n} \quad + C_3^{\frac{1}{3}} D_{n-2,1}, \\ C_1 . D_{\lambda,\mu} &= D_{\lambda+1,\mu} + D_{\lambda,\mu+1} + C_3 D_{\lambda-1,\mu-1}, \end{aligned}$$

for which $\lambda + \mu = n - 1$ suffice to determine the $n + 1$ forms of order $3(n+1)$ in the ξ's. But the statement is easily seen to be true for $n = 1$ and for $n + 3$. It is therefore true generally.

THEOREM XIII.—*If* $t \not\equiv 0$ (*mod* 3), *the full system of the group* $\{T_1, T_2, S, s\}$ *is* C_1, C_2, $C_3^{\frac{1}{N_1}}$; *if* $t \equiv 0$ (*mod* 3), *it is* C_1, C_2, $C_3^{\frac{1}{N_1}}$, D.

Between the four forms of the full system C_1, C_2, $C_3^{\frac{1}{N_1}}$, D, there exists the single relation

$$D^3 = 3C_2 . D + 9C_3 + C_1C_2 + 3C_3^{\frac{1}{3}}(2C_2 + C_1D) + 3C_3^{\frac{2}{3}}(D + 2C_1). \quad (106)$$

§15.—*The Invariant Forms of the Group* $\{T_1, T_2, S, s, \tau\}$.

To find the full system of the group $\{T_1, T_2, S, s, \tau\}$, one has only to impose proper conditions upon the exponents occurring in the system of Theorem XII, and to add such products, two at a time, of forms belonging to the group $\{T_1, T_2, S, s\}$ as undergo no change except a change of sign when operated upon by τ.

The systems of invariants of Theorem XII, written out in full, are

for $t \not\equiv 0$ (mod 3),

$$\Sigma z_1^{\kappa N_1}, \quad \Sigma z_1^{\lambda N_1} z_2^{\mu N_1}, \quad (z_1 z_2 z_3)^\nu; \quad (107)$$

for $t \equiv 0$ (mod 3),

$$\Sigma z_1^{\kappa N_1}, \quad \Sigma z_1^{\vartheta''(n+3\lambda)} z_2^{\vartheta''(2n+3\mu)}, \quad n = 0, 1, \quad (z_1 z_2 z_3)^\nu. \quad (108)$$

The conditions to be imposed, as is easily seen, are given by the following tables:

I. $t \not\equiv 0 \pmod 3$:

$$1).\quad N_1 \text{ even} \begin{cases} (\alpha) & \tau = \tau_4, \quad \nu \equiv 0 \pmod 2, \\ (\beta) & \tau \not\equiv \tau_4, \quad \nu = 0 \pmod 2. \end{cases}$$

$$2).\quad N_1 \text{ odd} \begin{cases} (\alpha) & \tau = \tau_4, \quad \varkappa \equiv \lambda + \mu \equiv \nu \equiv 0 \pmod 2, \\ (\beta) & \tau \not\equiv \tau_4, \quad \varkappa \equiv \lambda \equiv \mu \equiv \nu \equiv 0 \pmod 2. \end{cases}$$

II. $t \equiv 0 \pmod 3$:

$$1).\quad N_1 \text{ even} \begin{cases} (\alpha) & \tau = \tau_4, \quad \nu \equiv 0 \pmod 2, \\ (\beta) & \tau \not\equiv \tau_4, \quad \nu \equiv 0 \pmod 2. \end{cases}$$

$$2).\quad N_1 \text{ odd} \begin{cases} (\alpha) & \tau = \tau_4, \quad \varkappa \equiv n + \lambda + \mu \equiv \nu \pmod 2, \\ (\beta) & \tau \not\equiv \tau_4, \quad \varkappa \equiv n + \lambda \equiv \mu \equiv \nu \pmod 2. \end{cases}$$

If, as before, the substitution $z_i^{\vartheta''} = \xi_i$ be made, the results obtained may be given by the following:

Theorem XIV.—*The invariant forms of the group* $\{T_1, T_2, S, s, \tau\}$ *are—*

for $t \not\equiv 0 \pmod 3$,

$$\Sigma\xi_1^{3\kappa}, \quad \Sigma\xi_1^{3\lambda}\xi_2^{3\mu}, \quad (\xi_1\xi_2\xi_3)^\nu,$$

the exponents subject to the conditions of table I;

for $t \equiv 0 \pmod 3$,

$$\Sigma\xi_1^{3\kappa}, \quad \Sigma\xi_1^{\vartheta''(n+3\lambda)}\xi_2^{\vartheta''(2n+3\lambda)}, \quad (n = 0, 1), \quad (\xi_1\xi_2\xi_3)^\nu,$$

the exponents subject to the conditions of Table II, and in both cases when $\tau = \tau_4$, *the products composed of an even number of factors of odd order invariant with respect to the group* $\{T_1, T_2, S, s\}$ *must be added.*

§16.—*The Full Systems for the Group* $\{T_1, T_2, S, s, \tau\}$.

In order to abbreviate the work of finding the full systems for the cases given above, the following notation, part of which has already been used, will be adopted. We put

$$\left.\begin{array}{lll} C_1 = \Sigma\xi_1^3, & C_2 = \Sigma\xi_1^3\xi_2^3, & C_3 = (\xi_1\xi_2\xi_3)^3, \\ D = \Sigma\xi_1\xi_2^2, & E = \Sigma\xi_1^4\xi_2^2, & F = \Sigma\xi_1\xi_2^5, \\ G = \Sigma\xi_1^6\xi_2^6, & K = (\xi_1\xi_2\xi_3)^{\frac{3}{N_1}}, & \Sigma\xi_1^3 = C_3^{\frac{1}{N_1}}.C_1, \\ L = C_1^{\frac{1}{N_1}}.D, & S_2 = \Sigma\xi_1^6, & M = C_3^{\frac{1}{N_1}}.D. \end{array}\right\} \qquad (109)$$

Cases 1) and 2). $t \not\equiv 0 \pmod 3$, N even, τ any τ.

The full system for both cases is clearly

$$C_1, \quad C_2, \quad C_3^{\frac{2}{N_1}}. \tag{110}$$

Case 3). N_1 odd, $t \not\equiv 0 \pmod 3$, $\tau = \tau_4$.

The forms belonging to the group $\{T_1, T_2, S, s, \tau\}$ are also invariant with respect to the group $\{T_1, T_2, S, s\}$. Every invariant of the latter group is expressible rationally in terms of C_1, C_2, $C_3^{\frac{1}{N_1}}$. This fact may be expressed by the equation

$$\phi(z_1, z_2, z_3) = \Sigma m_{\alpha,\beta,\gamma} C_1^\alpha C_2^\beta C_3^{\frac{\gamma}{N_1}}.$$

The form C_2 is an invariant of the group $\{T_1, T_2, S, s, \tau\}$. The even powers of C_1 and $C_3^{\frac{1}{N}}$ are expressible in terms of C_2, $C_3^{\frac{2}{N_1}}$ and $S_2 = \Sigma \xi_1^6$. It follows immediately that ϕ is expressible rationally in terms of

$$C_2, \quad C_3^{\frac{2}{N_1}}, \quad S_2 \text{ and } K, \tag{111}$$

and it is apparent that these forms (111) constitute the full system. Between the forms of the full system there exists the single relation

$$K^2 = C_3^{\frac{2}{N_1}}(S_2 + 2C_2). \tag{112}$$

4). $t \not\equiv 0 \pmod 3$, N_1 odd, $\tau \neq \tau_4$.

Since the conditions are $\kappa \equiv \lambda \equiv \mu \equiv \nu \equiv 0 \pmod 3$, the system of forms is given by

$$\Sigma(\xi_1^2)^{3\kappa}, \quad \Sigma(\xi_1^2)^{3\lambda}(\xi_2^2)^{3\mu}, \quad \sqrt[\delta'']{(\xi_1^2\xi_2^2\xi_3^2)^\nu}.$$

It is at once evident that the full system is

$$S_2, \quad G, \quad C_3^{\frac{2}{N_1}}. \tag{113}$$

5) and 6). $t \equiv 0 \pmod 3$, N_1 even, $\tau = \tau_4$ or $\tau \neq \tau_4$.

The system of forms differs from the system of the group $\{T_1 T_2 S, s\}$ only in the exclusion of odd powers of $C_3^{\frac{1}{N_1}}$. The forms $\Sigma\xi_1^{3\kappa}$, $\Sigma\xi_1^{n+3\lambda}\xi_2^{2n+3\mu}$ are expressible in terms of C_1, C_2, C_3, and C_3 is, in the present case, an even power of $C_3^{\frac{1}{N_2}}$. Therefore, the full system is

$$C_1, \quad C_2, \quad D, \quad C_3^{\frac{2}{N_1}}. \tag{114}$$

The relation existing between the four forms (114) is the relation (106) which may be written in the form

$$D^3 = 3C_2D + 9\left(C_3^{\frac{2}{N_1}}\right)^{\frac{N_1}{2}} + C_1C_2 + 3\left(C_3^{\frac{2}{N_1}}\right)^{\frac{N_1}{6}}(2C_2 + C_1D)$$
$$+ 3\left(C_3^{\frac{2}{N_1}}\right)^{\frac{N_1}{3}}(D + 2C_1). \qquad (115)$$

7). $t \equiv 0 \pmod 3$, N_1 odd, $\tau = \tau_4$.

By a process similar to that used in 3), it is found that the forms of the system may be expressed rationally in terms of the seven forms

$$C_1^2, \quad C_1D, \quad C_1C_3^{\frac{1}{N_1}}, \quad C_2, \quad D^2, \quad C_3^{\frac{1}{N_1}}D \text{ and } C_3^{\frac{2}{N_1}}.$$

Between these forms and the forms E, F, K and S_2, there exist the following relations:

$$\left.\begin{aligned} C_1^2 &= S_2 + 2C_2, \\ C_1D &= E + F + C_3^{\frac{1}{3}-\frac{1}{N_1}}.L, \\ D^2 &= E + 2C_3 + 2C_2^{\frac{1}{3}-\frac{1}{N_1}}(K + L) + 6C_3^{\frac{3}{3}}, \end{aligned}\right\} \qquad (116)$$

By means of the relations (116), the forms C_1^2, CD, D^2 may be replaced by S_2, F, G respectively. No other relations of the sixth order in the ξ's exist. We may then choose for the full system the forms

$$S_2, \quad C_2, \quad C_3^{\frac{2}{N_1}}, \quad E, \quad F, \quad K, \quad L. \qquad (117)$$

The following relations hold for the forms (117):

$$\left.\begin{aligned} K^2 &= C_3^{\frac{2}{N_1}}(S_2 + 2C_2), \\ L^2 &= C_3^{\frac{2}{N_1}}\left[E + 2C_2 + 2C_3^{\frac{N_1}{2}\cdot\frac{N_1-3}{2}}(K + L) + 6C_3^{\frac{2}{3}}\right], \\ E^3 &= S_2\left(C_2^2 + 3C_3^{\frac{2}{3}}.E + 6C_3^{\frac{4}{3}}\right) \\ &\quad - 2C_3^{\frac{2}{N_1}\left(\frac{N_1-1}{2}\right)}K\left(3E + S_2 + 3C_3^{\frac{2}{3}}\right) \\ &\quad + 3C_3^{\frac{2}{3}}\left(3C_3^{\frac{2}{3}} + C_3^{\frac{2}{3}}E + 2C_2^2\right) + 3C_2^2E, \\ F^2 &= \left[E + 2C_2 + 2C_3^{\frac{2}{N_1}\cdot\frac{N_1-3}{6}}(K + L) + 6C_3^{\frac{2}{3}}\right] \\ &\quad \times\left[S_2 + 2C_2 + C_3^{\frac{8}{3}} - 2C_3^{\frac{2}{N_1}\cdot\frac{N_1-3}{6}}K\right] - E(E + 2F). \end{aligned}\right\} \qquad (118)$$

8). $t \equiv 0 \pmod 3$, N_1 odd, $\tau \not\equiv \tau_4$.

For $n \overline{\gtrless} 2$ the $n+1$ equations

$$\Sigma\xi_1^6, \quad \Sigma\xi_1^{1+3(2\lambda+1)}\xi_2^{6\mu} = \Sigma\xi_1^{1+3(2\lambda+3)}\xi_2^{2+6\mu} + \Sigma\xi_1^{1+3(2\lambda+1)}\xi_2^{2+6(\mu+1)} + C_3^{\frac{2}{3}}\Sigma\xi_1^4\xi_2^{2+6\lambda}\xi_3^{6\mu},$$

$$\lambda = 0, 1, 2, 3 \ldots\ldots n-1, \quad \lambda + \mu = n-1,$$

$$\Sigma\xi_1^6\xi_2^6 . \Sigma\xi_1^4\xi_2^{6(n-2)} = \Sigma\xi_1^4\xi_2^{2+6(n-1)} + C_3^{\frac{2}{3}}\Sigma\xi_1^{2+6(n-2)} + C_3^{\frac{2}{3}} . \Sigma\xi_1^4\xi_2^8\xi_2^{6(n-2)}$$

suffice to determine the $n+1$ forms

$$\Sigma\xi_1^{1+3(2\lambda+1)}\Sigma\xi_2^{2+6\mu}, \qquad \lambda = 0, 1, 2 \ldots\ldots n, \quad \lambda + \mu = n,$$

of order $6(n+1)$ in the ξ's in terms of the forms of order $6n$ or lower. It is easily shown that the forms of orders 8 and 12 in the ξ's are expressible in terms of the forms

$$S_2, \quad G, \quad E, \quad C_3^{\frac{2}{N_1}}. \tag{119}$$

It follows immediately that these four forms constitute the full system.

The four forms of the full system are bound by the relation

$$E^3 = 3EG + 9C_3^2 + S_2G + 3C_3^{\frac{2}{3}}(2G + S_2E) + 3C_3^{\frac{4}{3}}(E + 2S_2). \tag{120}$$

The results just obtained give the following:

THEOREM XV.—*The full system of the groups* $\{T_1, T_2, S, s, \tau\}$ *are given as follows:*

For $t \not\equiv 0 \pmod 3$:

1) N_1 *even*, $\tau = \tau_4$, C_1, C_2, $C_3^{\frac{2}{N_1}}$.

2) " $\tau \not\equiv \tau_4$, C_1, C_2, $C_3^{\frac{2}{N_1}}$.

3) N_1 *odd*, $\tau = \tau_4$, S_2, C_2, $C_3^{\frac{2}{N_1}}$, K.

4) " $\tau \not\equiv \tau_4$, S_2, G, $C_3^{\frac{2}{N_1}}$.

For $t \equiv 0 \pmod 3$:

5) N_1 *even*, $\tau = \tau_4$, C_1, C_2, D, $C_3^{\frac{2}{N_1}}$.

6) " $\tau \not\equiv \tau_4$, C_1, C_2, D, $C_3^{\frac{2}{N_1}}$.

7) N_1 *odd*, $\tau = \tau_4$, S_2, C_2, $C_3^{\frac{2}{N_1}}$, E, F, K, L.

8) " $\tau \not\equiv \tau_4$, S_2, G, E, $C_3^{\frac{2}{N_1}}$.

where the forms C_1, C_2, C_3, E, F, G, K, L, S_2 *are defined by* (109).

The relations existing in those cases where more than three forms belong to the full system are, for case 3), (112) ; *for cases* 5) *and* 6), (115) ; *for case* 7, (118) ; *for case* 8), (120)

CHAPTER III.

The Orders of the Principal Ternary Monomial Groups.

§17.—*The Order of the Group* $\{T_1, T_2, S\}$.

Let $\quad U_i = ST_iS^{-1} = (\omega_{N_i}^{k_2}, \omega_{N_i}^{k_3}, \omega_{N_i}^{k_1}), \qquad i = 1, 2.$

The substitution U_2 belongs to the group $\{T_1, T_2\}$, for, from the condition

$$T_1^{\alpha} T_2^{\beta} = U^{\delta},$$

one has for the determination of α, β, δ the two independent congruences

$$\left.\begin{aligned} \bar{N} k_2'\delta &\equiv k_1\alpha + \bar{N} k_1'\beta, \\ \bar{N} k_2\delta &\equiv k_2\alpha + \bar{N} k_2'\beta, \end{aligned}\right\} \pmod{N_1}. \tag{121}$$

The congruences (121) reduce at once to

$$\left.\begin{aligned} k_1\alpha_1 + k_1'\beta &\equiv k_2'\delta, \\ k_2\alpha_1 + k_2'\beta &\equiv k_3'\delta, \end{aligned}\right\} \pmod{N_2}, \tag{122}$$

where $\alpha = \alpha_1\bar{N}$.

By hypothesis $[(k_1 k_2'), N_2] = 1$, so that one may find α_1 and β from (122) whatever value may be assigned to δ. We have then

$$U_2 = T_1^{\alpha} T_2^{\beta},$$

where α and β are the solutions of the congruences (121) when $\delta = 1$.

The conditions that U_1^{δ} is found in the group $\{T_1, T_2\}$ reduce to

$$\left.\begin{aligned} k_2\delta - k_1\alpha &\equiv 0, \\ k_3\delta - k_2\alpha &\equiv 0. \end{aligned}\right\} \pmod{\bar{N}}. \tag{123}$$

But the solution of (123) has already been found, since these congruences are identical with (27). If we make $\bar{\mathfrak{S}} = Qr$, this solution is

$$\left.\begin{aligned} \alpha &= \bar{\mathfrak{S}}(n + \lambda t), \\ \delta &= -\bar{\mathfrak{S}}(v_n + \mu t), \\ vk_2 + k_1 &\equiv 0 \pmod{t}, \\ v_n &\equiv nv \pmod{t}, \end{aligned}\right\} \tag{124}$$

or

$$\left.\begin{aligned} \alpha &= \bar{\mathfrak{S}}(w_n + \lambda' t), \\ \delta &= -\bar{\mathfrak{S}}(n + \mu' t), \\ wk_1 + k_2 &\equiv 0 \pmod{t}, \\ w_n &\equiv nw \pmod{t}. \end{aligned}\right\} \tag{125}$$

To find the least positive value δ satisfying (123), one may put $n = t - 1$ and $\mu' = 1$ in (125). The value for δ and the corresponding values for α, say α_s and δ_s, are then

$$\begin{aligned} \delta_s &= \bar{\mathfrak{S}}, \\ \alpha_s &= \bar{\mathfrak{S}}(w_{t-1} + \lambda t). \end{aligned} \tag{126}$$

It may be proven that values for λ and β exist both $\overline{\gtrless} N_2$, which will satisfy the conditions for

$$U_1^\delta = T_1^\alpha T_2^\beta,$$

where δ_s and α_s are substituted for δ and α respectively. It follows that the order of the group

$$\{T_1, T_2, U_1, U_2\} \text{ is } N_1 N_2 \bar{\mathfrak{S}}.$$

To find the order of the group $\{T_1, T_2, S\}$, we have

$$ST_i^\alpha = U_i^\alpha S, \qquad i = 1 \text{ or } 2.$$

Let $$SU_i^\alpha S^{-1} = V_i^\alpha,$$
whence $$S^2 T_i^\alpha S^{-2} = V_i^\alpha$$
and $$S^2 T_i^\alpha = V_i^\alpha S^2.$$

But $T_i U_i V_i = 1$, since $\Sigma k \equiv 0 \pmod{N_1}$ and $\Sigma k' \equiv 0 \pmod{N_2}$.

Therefore, $$V_i^\alpha \equiv T_i^{-\alpha} U_i^{-\alpha}$$
and $$S^2 T_i^\alpha = T_i^{-\alpha} U_i^\alpha S_1^2.$$

It follows that every element of the group $\{T_1, T_2, S\}$ may be put in the form

$$\begin{aligned} &T_1^\alpha T_2^\beta U_1^\gamma S^\delta, \\ &\alpha = 0, 1, 2 \ldots\ldots N_1 - 1, \\ &\beta = 0, 1, 2 \ldots\ldots N_2 - 1, \\ &\gamma = 0, 1 \quad \ldots\ldots \bar{\mathfrak{S}} - 1, \\ &\delta = 0, 1, 2. \end{aligned}$$

Therefore, the order of the group $\{T_1, T_2, S\}$ is

$$3N_1 N_2 \bar{\mathfrak{S}} = 3NQr.$$

§18.—*The Order of the Group* $\{T_1, T_2, s\}$.

If by s we mean the substitution (i, l), and if we put

$$sT_1s = u_{il}\ ,\quad sT_2s^{-1} = v_{il},$$

so that
$$s\,u_{il}\,s^{-1} = T_1,\quad s\,v_{il}\,s^{-1} = T_2,$$

it may be seen that every substitution of the group $\{T_1, T_2, s\}$ may be put in the form

$$T_1^{\alpha}\,T_2^{\beta}\,u_{il}^{\gamma}\,v_{il}^{\delta}\,s^{\epsilon}.$$

We have then to find the lowest powers of u_{il} and v_{il} that occur in the group $\{T_1, T_2\}$.

The group $\{T_1, T_2\}$ contains the substitution v_{il}, for suppose

$$T_1^{\alpha}\,T_2^{\beta} = v_{il}^{\gamma},$$

From this condition

$$\left.\begin{aligned} k_i\,\alpha + \bar{N}k_i'\beta &\equiv \bar{N}\,k_l'\gamma,\\ k_j\,\alpha + \bar{N}\,k_j'\beta &\equiv \bar{N}\,k_j\gamma.\end{aligned}\right\}\ (\text{mod}\ N_1), \tag{127}$$

If $\alpha = \bar{N}_1\,\alpha_1$, the congruences (127) reduce to

$$\left.\begin{aligned} k_i\,\alpha_1 + k_i'\,\beta &\equiv k_l'\,\gamma,\\ k_j\,\alpha_1 + k_j'\,\beta &\equiv k_j'\gamma.\end{aligned}\right\}\ (\text{mod}\ N_2). \tag{128}$$

The congruences (128) have a solution for any value of γ, since $[(k_i, k_j), N_2] = 1$, hence for $\gamma = 1$.

To find the lowest power of u_{il} contained in $\{T_1, T_3\}$, let

$$T_1^{\alpha}\,T_2^{\beta} = u_{il}^{\gamma}.$$

We have then the two independent congruences

$$\left.\begin{aligned} k_i\,\alpha - k_l\,\gamma &\equiv \bar{N}k_i'\beta,\\ k_j\,\alpha - k_j\,\gamma &\equiv \bar{N}\,k_j'\beta.\end{aligned}\right\}\ (\text{mod}\ N_1). \tag{129}$$

From (129) follow, as necessary conditions,

$$\left.\begin{aligned} k_i\,\alpha - k_l\gamma &\equiv 0,\\ k_j\,\alpha - k_j\gamma &\equiv 0.\end{aligned}\right\}\ (\text{mod}\ \bar{N}). \tag{130}$$

By (65) and (67) we have

$$k_j = q_j\,k_j,\quad k_i - k_l = s't',\quad \bar{N} = QPr't'.$$

With this notation, the solution of (130) is found to be

$$\begin{aligned} \gamma &= Q_j Pr' (n + \lambda q_j t'), \\ \alpha &= Q_j Pr' (-w''_n + \mu q_j t'), \\ w'' k_i + k_l &\equiv 0 \pmod{q_j t'}, \\ w''_n &\equiv n w'' \pmod{q_j t'}. \end{aligned}$$

The least value of γ and the corresponding value of α are therefore

$$\begin{aligned} \gamma &= Q_j Pr', \\ \alpha &= Q_j Pr' (t' - w'' + \mu q_j t'): \end{aligned}$$

These values satisfy both the congruences (130), and with them substituted in (129) it may be shown that there exist a set of values for μ and β both $\overline{\gtrless} N_2$, which will satisfy (129). It follows that $\mu_{il}^{Q_j Pr'}$ is the lowest power of u_{il} occurring in the group $\{T_1, T_2, u_{il}, v_{il}\}$, and that the order of this group is $N_1 N_2 Q_j Pr'$.

Every substitution of the group $T_1, T_2, s_{il}\}$ may be put in the form

$$\begin{aligned} &T_1^{\alpha} T_2^{\beta} u_{il}^{\gamma} s_{il}^{\delta} \\ &\alpha = 0, 1, \dots\dots N_1 - 1, \\ &\beta = 0, 1, \dots\dots N_2 - 1, \\ &\gamma = 0, 1, \dots\dots Q_j Pr, \\ &\delta = 0, 1. \end{aligned}$$

The order of the group $\{T_1, T_2, s_{il}\}$ is therefore

$$2NQ_j Pr' = 2N \frac{\bar{N}}{q_j t'}.$$

§19.—*The Order of the Group* $\{T_1, T_2, s_{i\kappa}, \tau\}$.

The substitutions τ_j and τ_4 are interchangeable with all the substitutions of the group $\{T_1, T_2, s_{i\kappa}\}$, and the order of the group $\{T_1, T_2, s_{i\kappa}, \tau\}$ is therefore $2^2 N \frac{\bar{N}}{q_j t'}$.

If τ is τ_i, let
$$\theta_\lambda = T_1^{\alpha} T_2^{\beta} u_{i\kappa}^{\gamma} s_{i\kappa}^{\delta}$$

be any substitution of the group $\{T_1, T_2, s_{i\kappa}\}$, and let $s = 2N \frac{\bar{N}}{q_j t'}$. $\tau_i \theta_\lambda$ is either

$\theta_\lambda \tau_i$ or $\theta_\lambda \tau_\kappa$ according as δ is 0 or 1. We may then form the following table:

$$\begin{array}{llll} \theta_1 = 1, & \theta_2, & \theta_3, \ldots & \theta_\rho, \\ \tau_i, & \theta_2\tau_i, & \ldots & \theta_\rho\tau_i, \\ \tau_l, & \theta_2\tau_l, & \ldots & \theta_\rho\tau_l, \\ \tau_i\tau_l, & \theta_2\tau_i\tau_l, & \ldots & \theta_\rho\tau_i\tau_l. \end{array}$$

If N_1 is even, the first line contains one of the substitutions $\sigma_1, \sigma_2, \sigma_3$, (51) viz. $T_1^{\frac{N_1}{2}}$.

Suppose $T_1^{\frac{N_1}{2}} = \sigma_i$, then σ_i and $\sigma_l = s_{i\kappa}\sigma_i s_{il}$ and, consequently, $\sigma_j = \sigma_i\sigma_l = \tau_i\tau_l$ are found in the first line of the table. The group is then exhausted by the first two lines of the table. The same argument applies when $T_2^{\frac{N_1}{2}}$.

If $T_1^{\frac{N_1}{2}} = \sigma_j$, the first line contains neither σ_i nor σ_κ, unless N_2 is also even, since $s_{il}\sigma_j s_{il} = \sigma_j$. The second line contains $\sigma_j\tau_i = \tau_l$ and $\tau_i\tau_l = \sigma_j$ is contained n the first line. The group is then exhausted by the first two lines.

If N_1 is odd, the group contains τ_i and $s_{il}\tau_i s_{il} = \tau_l$ which are not found in the first line, and $\tau_i\tau_l = \sigma_j$ which is not found in any one of the first three lines. In this case the order of the group is $2^3 N_1 N_2 \dfrac{\bar{N}}{q_j t'}$.

The same argument holds for $\tau = \tau_l$.

The final result is, the order of the group $\{T_1, T_2, s_{il}, \tau\}$ is $2^2 N \dfrac{\bar{N}}{q_j t'}$, unless N_1 is odd and τ is either τ_i or τ_l, in which cases it is $2^3 N \dfrac{\bar{N}}{q_j t'}$.

§20.—*The Order of the Group* $\{T_1, T_2, S, s\}$.

The group $\{T_1, T_2, S\}$ is a self-conjugate subgroup of the group $\{T_1, T_3, S, s\}$. It follows immediately, since s is of order two, that the order of the latter is twice that of the former.

The order of the group $\{T_1, T_2, S, s\}$ is $2 \cdot 3 \cdot NQr$.

§21.—*The Order of the Group* $\{T_1, T_2, S, s, \tau\}$.

There are two cases:

Case I. $\tau = \tau_4$.

The substitution τ_4 is interchangeable with every substitution of the group $\{T_1, T_2, S, s\}$, hence the order of the group in question is $2^2 \cdot 3NQr$.

Case II. $\tau \neq \tau_4$.

Subcase 1). If N_1 is even, $\{T_1, T_2, S, s\}$ contains one of the substitutions σ, namely, $T_1^{\frac{N_1}{2}}$ and, consequently, it contains $\sigma_1, \sigma_2, \sigma_3$. Moreover, the substitutions of $\{T_1, T_2, S, s\}$ may be put in the forms

$$T_1^\alpha T_2^\beta U^\gamma S^\delta s^\epsilon \text{ or } T_1^\alpha T_2^\beta U^\gamma \theta_\lambda,$$

where θ_λ is one of the six substitutions of the group $\{S, s\}$. We have

$$\theta_\lambda^{-1} \tau_i \theta_\lambda = \tau_\mu,$$

hence

$$\tau_i \theta_\lambda = \theta_\lambda \tau_\mu.$$

It follows that the substitutions of the group $\{T_1, T_2, S, s, \tau\}$ may all be put in one of the four forms R_ν, $R_\nu \tau_1$, $R_\nu \tau_2$, $R_\nu \tau_3$, where $\nu = 1, 2, 3 \ldots\ldots 2 \,.\, 3 N_1 N_2 Q^r$ are the substitutions of the group $\{T_1, T_2, S, s\}$.

But

$$R_\nu = R_\nu \sigma,$$

whence

$$R_\nu \tau_1 = R_\nu \sigma_1 \tau_1 = R_\nu \tau_2 = R_\nu \tau_3,$$

so that the group is exhausted by the sets R_{ν_1} and $R_\nu \tau_1$. The order is, therefore, $2^2 \,.\, 3 N_1 N_2 Q r$.

Subcase 2). If N_1 is odd, the substitutions R_ν, $R_\nu \tau_1$, $R_\nu \tau_2$, $R_\nu \tau_3$ are all distinct, since otherwise one would have

$$R_{\nu_1} \tau_i = R_{\nu_2} \tau_j,$$

whence

$$R_{\nu_1}^{-1} R_{\nu_2} = \tau_i \tau_j = \sigma_\kappa,$$

but σ_κ cannot occur in the set R_ν. Hence the order of the group is $2^3 \,.\, 3 N Q r$. The result may be stated as follows: If $\tau = \tau_4$, or if $\tau \neq \tau_4$ and N_1 is even, the order of the group $\{T_1, T_2, S, s, \tau\}$ is $2^2 \,.\, 3 \,.\, N Q r$; if $\tau \neq \tau_4$ and N_1 is odd, the order is $2^3 \,.\, 3 \,.\, N \,.\, Q r$.